TRUCOS WINDOWS: RESOLVER PROBLEMAS DE APAGADO

@RROBA

123
AÑO X

SÓLO 4,95€

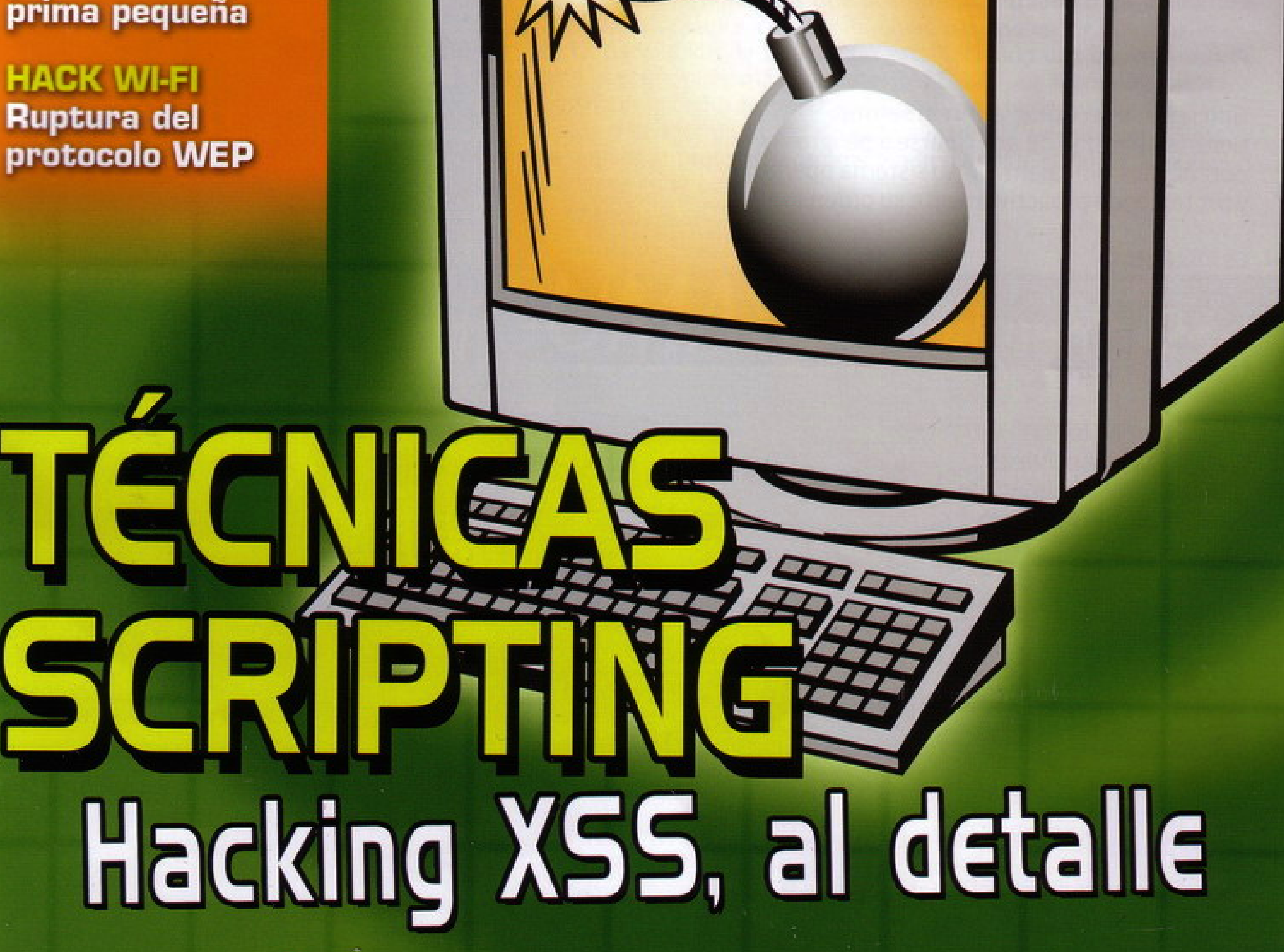
8 414090 201599 00123

LA REVISTA ESPAÑOLA MÁS VETERANA DE INTERNET Y SEGURIDAD INFORMÁTICA

DESAFÍO BACKTRACK
La distro de Linux para seguridad

TRUECRYPT
Criptografía que podría usar tu prima pequeña

HACK WI-FI
Ruptura del protocolo WEP



TÉCNICAS SCRIPTING

Hacking XSS, al detalle

Y ADEMÁS...
Crack
Hacktivismo
Virus

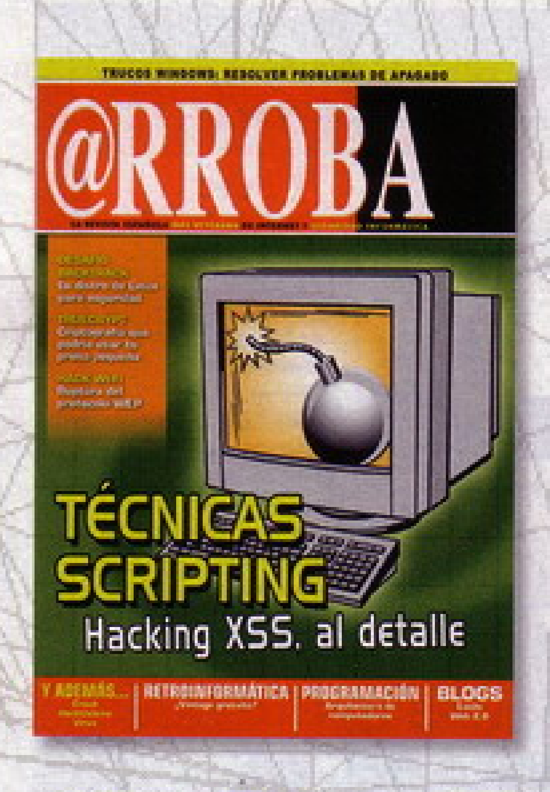
RETROINFORMÁTICA
¿Vintage gratuito?

PROGRAMACIÓN
Arquitectura de computadores

BLOGS
Estilo Web 2.0

@RROBA 123

NÚMERO 123 - www.megamultimedia.com/arroba



Patalear también

Los guionistas de Hollywood, en huelga; Bigas Luna, enfadado... En ambos casos, el origen del malestar es el mismo: Internet permite disfrutar de sus obras, y ellos no ven un céntimo. Los americanos se quejan porque los productores sí reciben ganancia por la explotación de sus guiones en Internet, DVD y otros medios tecnológicos. Bigas se preocupa por el P2P, e incluso contrata servicios para impedir la descarga de sus creaciones, aunque con escasa fortuna. En el fondo de todo, se percibe claramente la lucha por normalizar un sector que aún no ha encontrado su definición. Los internautas defendemos nuestro derecho a un acceso razonable a los contenidos culturales. La industria pretende, en cambio, obtener rendimiento económico de las posibilidades que ofrecen las nuevas tecnologías.

Es el momento de presionar para buscar una solución que no acabe perjudicándonos. En esta pelea, o nos organizamos, o acabamos con un control de contenidos que nos limitará el acceso hasta cotas insoportables. Contamos con los mimbres para defender nuestros intereses. La Asociación de Internautas está haciendo una buena labor, así como asociaciones más recientes: APEMIT, por ejemplo. Iniciativas personales, como la de David Bravo, nos han servido de gran ayuda para defender un punto de vista alejado de estereotipos. Bigas Luna se enfada y protesta; nosotros tendremos que patalear también o acabaremos en la cuneta.

SUMARIO número 123

PRESIDENTE DEL CONSEJO EDITORIAL MARICRUZ MONTOYA LINARES
COORDINADOR DE PRODUCCION FRANCISCO PEDREGAL BUENO
DIRECTOR CARLOS VERDIER
REDACTORES GABY LÓPEZ/ ANDRÉS MÉNDEZ/ CAROLINA GARCÍA/ MANUEL BALERIOLA/ NICOLÁS VELÁSQUEZ/ SET/ SS / SPARKRISP / MERCÈ MOLIST / FERNANDO GONT
MAQUETACIÓN: PABLO GUIL
@LGARROBA DIRIGE: GABY LÓPEZ
COORDINACIÓN DEPARTAMENTO GRÁFICO DEPARTAMENTO PROPIO
DPTO. DE SUSCRIPCIONES suscripciones@csr71.com

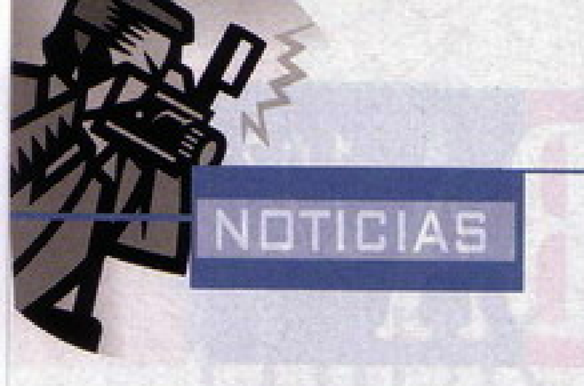
PUBLICIDAD: Central MEDIA Young/
BARCELONA
Avda. Meridiana 350, 12° C
08027 BARCELONA
Telf.: 93 274 47 39-Fax: 93 346 72 14
E-MAIL: central@cmy.es

@RROBA
arroba@megamultimedia.com
arroba2@megamultimedia.com
Megamultimedia, S.L.
Paseo de Reding, 43, 1°
29016 Málaga
Teléfono: 952 36 31 43

DISTRIBUIDORA INTERNACIONAL COEDIS

PRINTED IN SPAIN
XII/MMVII

ISSN-1138-1655 - Dep. legal MA-1049-97 / nº123



Arsys obtiene el certificado más exigente en seguridad

El proveedor de servicios de Internet Arsys Internet ha obtenido la certificación internacional 27001:2005 para su Sistema de Gestión de Seguridad de la Información. De este modo, Arsys Internet se incorpora al reducido número de empresas que tienen este certificado, el más exigente distintivo internacional en cuanto a eficacia y seguridad de la gestión de datos. Menos de veinte empresas españolas disponen de una certificación acreditada que constate el cumplimiento de esta normativa.

La confidencialidad, integridad y disponibilidad de la Información son los principales aspectos que supervisa este estándar internacional, aprobado en 2005 por la Organización Internacional para la Estandarización (ISO, por sus siglas en inglés).

La auditoría necesaria para conseguir el certificado ha sido realizada por Applus+, empresa acreditada por la Entidad Nacional de Certificación (ENAC) y una de las principales entidades de certificación del mercado internacional.

Según Manuel Amutio, Director General Técnico de Arsys Internet, "esta certificación supone un prestigioso reconocimiento al trabajo que realizamos desde hace más de once años. Este certificado implica compromiso permanente por parte de la empresa y también una garantía para nuestros clientes, cada vez más concienciados de la importancia que tiene la gestión de su información".

Esta certificación se suma a los distintos reconocimientos obtenidos por Arsys Internet, entre los que destaca la norma UNE-EN ISO 9001:2000 para las actividades de Diseño, Desarrollo y prestación de servicios de hosting, housing y registro de dominios.





Amen celebra el auge del comercio electrónico B2C en Españaconectividad inalámbrica de Conceptronic

Amen, líder en servicio y alojamiento en Internet en Europa, y pionera en la comercialización de soluciones integrales de comercio electrónico en España, Francia y Portugal, está celebrando los resultados positivos reflejados en los estudios sobre la evolución de la compra-venta online B2C dentro de nuestras fronteras.

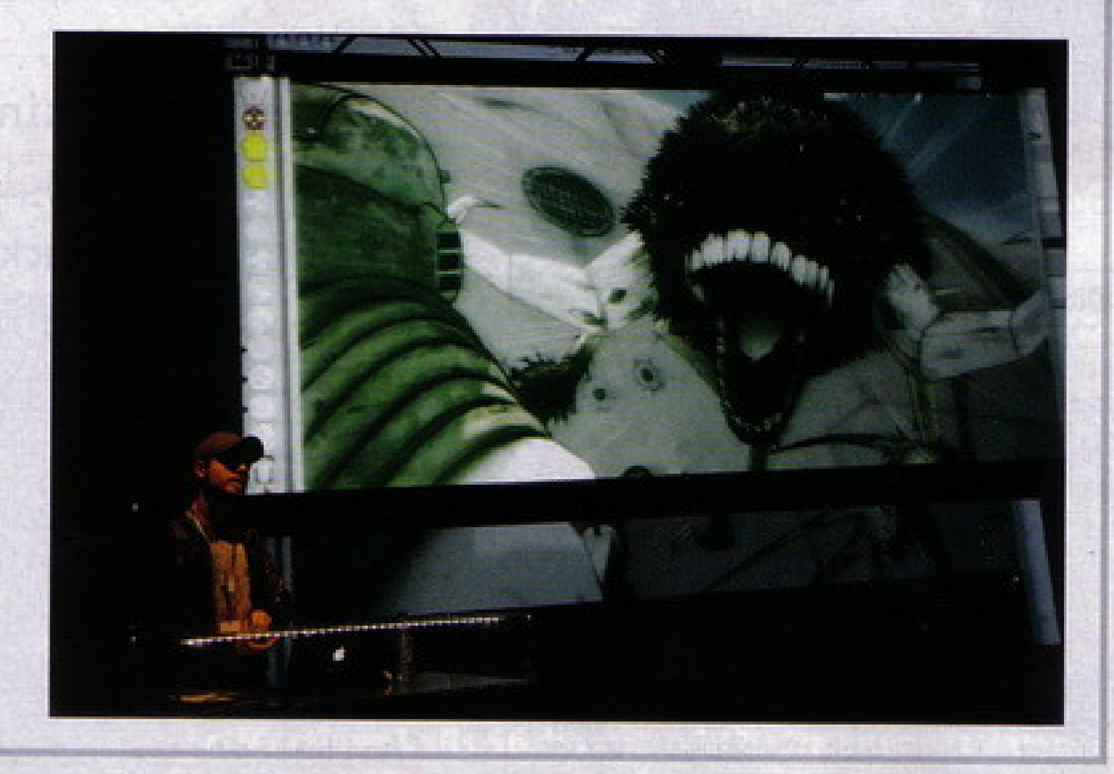
Los informes realizados por el Observatorio de las Telecomunicaciones y para la Sociedad de la Información de Red.es: "Comercio Electrónico B2C - 2007" y por el Instituto de Estadística demuestran que la práctica de realizar negocios por la Red se incrementó de forma importante entre los usuarios españoles durante el 2006. Más del 13% de la población mayor de 15 años se ha apuntado a esta modalidad y la practica de forma regular, lo que representa más de 5 millones de personas.

Amen participa en este incremento gracias al éxito de sus Packs e-Commerce. Desde su lanzamiento europeo en abril de este año, se han creado más de 1.800 tiendas online. Los packs e-Commerce incorporan un software de última generación altamente seguro y fiable para la creación de tiendas online profesionales de manera sencilla y rápida, acercando este modelo de negocio a las Pymes españolas.

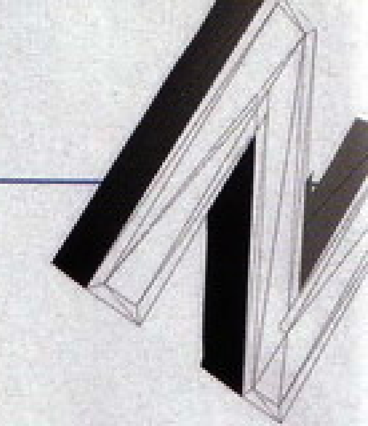
Artfutura 2007 continúa en Cádiz, Granada, Madrid, Valladolid, Vigo y Vitoria

ArtFutura, el festival de creación y cultura digital de referencia en España, ha clausurado su edición de Barcelona pero sus proyecciones continúan en Cádiz, Granada, Madrid, Valladolid, Vigo y Vitoria. La edición 2007 ha supuesto todo un despliegue de actividades en torno a la creatividad digital que se han presentado en museos y centros culturales de once ciudades.

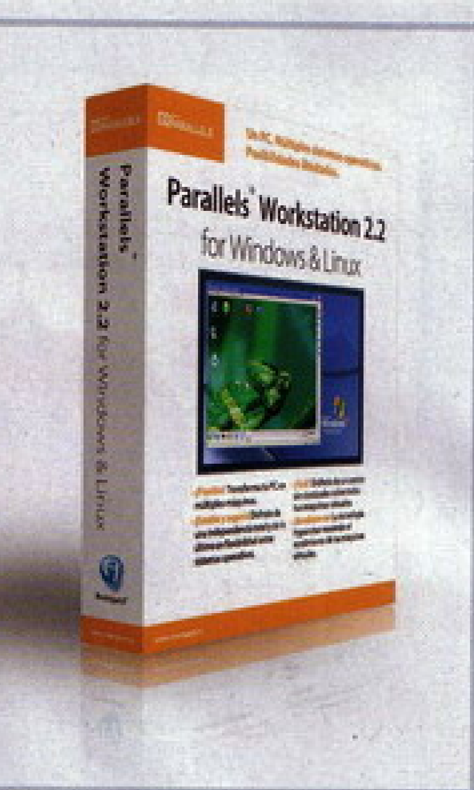
El centro neurálgico del festival ha estado en el Mercat de les Flors barcelonés. Allí, las presentaciones de proyectos como el innovador videojuego "Little Big Planet - uno de los títulos más esperados para el próximo 2008 - o la sesión dedicada al nuevo cine estereoscópico de Sony Pictures Imageworks sobre "Beowulf", no decepcionaron a un auditorio completamente lleno.







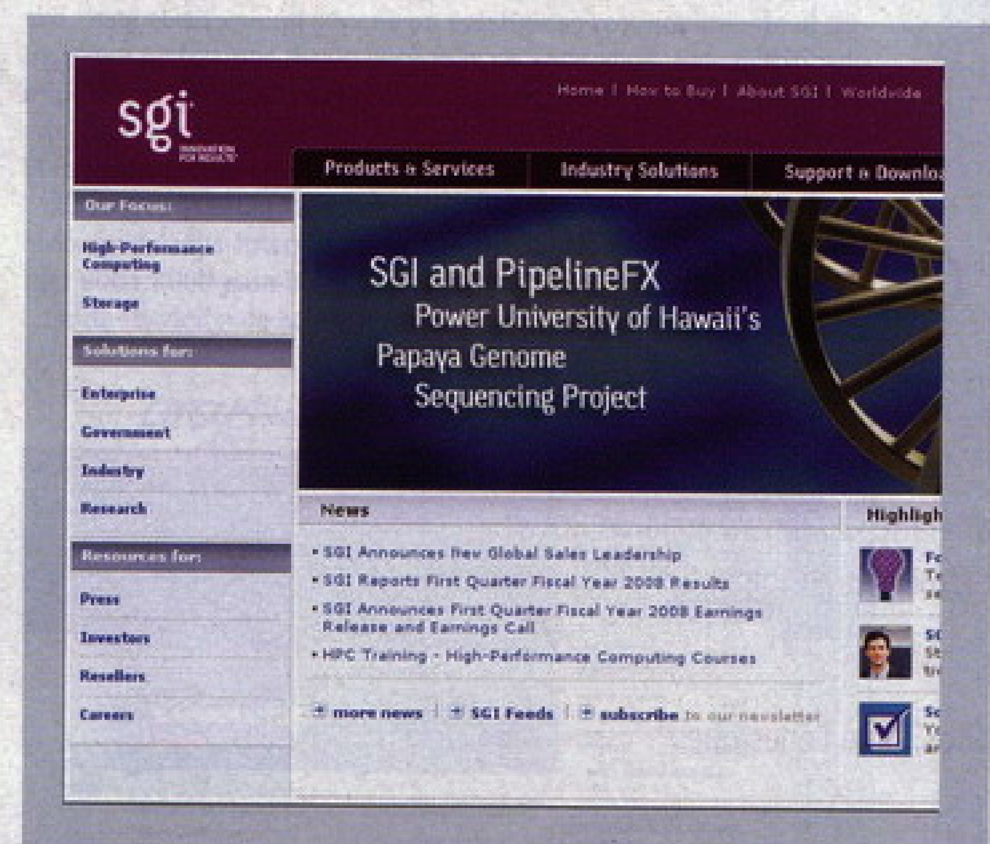
Parallels presenta Workstation 2.2 para Windows y Linux



Parallels, la compañía de software de virtualización de sobremesa con soluciones económicas y fáciles de usar, ha anunciado, a través de su editor en España, Avanquest Software, la próxima disponibilidad de Parallels Workstation 2.2 para Windows y Linux.

Parallels Workstation 2.2 permite a los usuarios ejecutar de forma simultánea cualquier versión de Windows, incluyendo Beta y RC builds de Windows Vista, cualquier distribución Linux, Solaris, FreeBSD, NetBSD, OpenBSD, OS/2, eComStation o DOS, en cualquier máquina virtual segura de cualquier ordenador que corra bajo Windows 2000, XP o 2003, o cualquier versión de Linux. No es necesario reiniciar ni particionar y los usuarios no necesitan apagar o abandonar su ordenador para acceder a una máquina virtual.

"Parallels Workstation 2.2 es un paso más en nuestra misión de diseñar las soluciones de virtualización más potentes y fáciles de usar del mercado", ha comentado Benjamin Rudolph, Director de Comunicación de SWsoft. "El conjunto de funcionalidades mejoradas y rendimiento, su incomparable sencillez de uso y un precio de mercado asequible convierte a Parallels Workstation 2.2 en la elección lógica para el usuario informático habitual que desea o necesita trabajar de forma simultánea con múltiples sistemas operativos".



Silicon Graphics cumple 25 años

Medicamentos y tratamientos de cáncer que han salvado vidas, automóviles y aviones más seguros y eficientes, vehículos de exploración espacial de siguiente generación, estudios del cambio climático, galardonados efectos especiales, nuevas formas de energía sostenible, tecnología para la Seguridad Nacional…son algunas de las innovaciones que se han llevado a cabo con la ayuda de SGI.

SGI conmemora su vigésimo quinto aniversario destacando cómo sus productos de computación, almacenamiento y visualización han permitido a sus clientes cambiar el mundo.

Fundada en 1982 por el profesor Jim Clark e ingenieros de la Universidad de Stanford, la compañía entregó su primer producto, un terminal gráfico, al año siguiente, a un cliente situado muy cerca de su sede en Mountain View, California: el Centro de Investigación Ames de la NASA.

"Año tras año, la NASA sigue confiando en los sistemas de SGI para generar conoc miento innovador acerca de nuestro planeta y su lugar en el universo," ha declarado F. Ron Bailey, Fundador y primer Jefe de la División de Supercomputación Avanzada de la NASA, situada en el Centro Ames.

Naciones Unidas, Google y Cisco presentan herramienta para luchar contra la pobreza

La Organización de Naciones Unidas (ONU), Google y Cisco han presentado un innovador sitio web que permite seguir los avances en la lucha contra la pobreza mundial hasta 2015, en el marco de la campaña mundial conocida como los Objetivos de Desarrollo del Milenio (ODM).

El Secretario General de las Naciones Unidas, Ban Ki-moon, presentó el proyecto, llamado MDG Monitor, y puso de relieve la necesidad urgente de aumentar la cooperación mundial.

"Alcanzar los Objetivos es una tarea realmente global que exige que los gobiernos, las organizaciones internacionales, las empresas privadas y las organizaciones no gubernamentales trabajen juntas", afirmó el Secretario General Ban Ki-moon. "Agradezco a Google y Cisco que nos hayan ayudado a crear el MDG Monitor, un ejemplo del tipo de alianzas innovadoras que necesitamos".

A la presentación del proyecto, una importante innovación en el seguimiento del avance del desarrollo, se sumaron el Secretario General el Administrador del PNUD (Programa de Desarrollo de Naciones Unidas) Kemal Dervi□; el Vicepresidente Mundial de Operaciones de Proveedores de Servicio de Cisco Systems Carlos Domínguez y el Jefe de Tecnología de Google Earth and Maps, Michael T. Jones.




Elige tu segundo idioma
Inglés o chino:
2 idiomas clave para moverse por el mundo y competir en el mercado laboral.
Si necesitas hablar inglés, el Profesor Maurer te ofrece la garantía de su famoso Método con el que más de 100.000 personas han aprendido a hablar inglés en sólo unos meses.
Y si lo que necesitas es hablar chino, con el eficaz método para personas que hablan español de la Profesora Yang Yun, lo aprenderás mucho más rápido de lo que piensas.
Elige tu segundo idioma e Infórmate.
CCC The Maurer Method
CCC Yang Yun System Chinese Course
902 20 21 22
www.cursosccc.com
Haz que las cosas pasen.
Para más información, envía este cupón a CCC: Apdo. 17222 - 28080 Madrid
Matricúlate este mes y consigue GRATIS esta estupenda AGENDA ELECTRÓNICA
Sí, deseo recibir información (*)
¿QUÉ CURSO TE INTERESA?
Nombre:
Apellidos:
E-mail:
Teléfono:
Fecha nacimiento:
Domicilio:
Nº:
Piso:
Población:
C.P.:
Provincia:
DNI (opcional):
País de nacimiento:
Profesor Maurer
Profesora Yang Yun



hack wifi

Laboratorio: Seguridad en el sistema de cifrado WEP VIII

Inyección de tráfico inalámbrico para la ruptura del protocolo WEP (Parte XIX)

A estas alturas ya han sido publicados varios artículos del Taller de Seguridad inalámbrica Hack Wi-Fi. A lo largo de estos artículos hemos ido estudiando el comportamiento, la seguridad, la inseguridad de esta tecnología sin cables. Hemos conocido y estudiado varias herramientas para la auditoria inalámbrica en diferentes sistemas operativos y hemos echado mano en varias ocasiones de la práctica para ensuciarnos las manos.

Estoy muy contento con el resultado de estos artículos. Son muchos los usuarios y lectores que me envían correos, visitan mi blog y hasta se registran en Wadalbertia para acercarse un poco más al mundo inalámbrico. También me comentan, que les han parecido muy útiles e interesantes todos los artículos de Hack Wi-Fi.

Algo la verdad, que me enorgullece y me alegra muchísimo. Esto quiere decir que he completado parte de los objetivos que perseguía. Gracias a todos por vuestros comentarios y opiniones. También aprovecho la ocasión, para incitar a todos aquellos lectores del Taller para que me envíen sus sugerencias y opiniones acerca del curso.

También es cierto, algo que ya sabía desde el principio que iba a ocurrir, que ya hemos tratado varios temas muy importantes y que considero básicos para seguir el Taller de redes inalámbricas. Hemos ido progresando poco a poco y ascendentemente el nivel del curso. Por ello, son varios los usuarios que se inician en el curso que me preguntan temas ya tratados por que se encuentran desorientados.

Por eso, en este artículo, citaré algunas noticias útiles para los iniciados. Material y documentos de interés que colocarán un poco "a los nuevos" y que les vendrán muy bien para adentrarse en las redes inalámbricas.

Lo primero, sin duda, es dirigiros a Wadalbertia, en el subforo Zona Inalámbrica (http://www.wadalbertia.org/phpBB2/viewforum.php?f=7) encontraréis material muy interesante. También podéis realizar aquí todas las preguntas que se os ocurran.

¿En cuanto a Material inalámbrico?.

VOY A COMENTAR ALGUNAS LIVE-CDS QUE VIENEN CARGADAS DE MATERIAL MUY ÚTIL PARA LA AUDITORIA INALÁMBRICA, ASÍ COMO CONTROLADORES PARA VARIAS TARJETAS INALÁMBRICAS

Pues voy a comentar algunas Live-CDs que vienen cargadas de material muy útil para la auditoria inalámbrica, así como controladores para varias tarjetas inalámbricas.

Para que os ahorréis tiempo en ir instalando y compilando todas las herramientas ya citadas en Hack Wi-Fi.

Aunque ya hablaremos más adelante y más profundamente de las Live-CDs, para la auditoria inalámbrica, aquí os dejas las más populares he interesantes.

BlackTrack 2

Esta Live-CD la podéis descargar de la siguiente url, Remote-Exploit.org

http://www.remote-exploit.org/backtrack_download.html

Interesante Live-CD ya no solo para la auditoria inalámbrica, sino para el Hacking en general.

WiFiWay 0.8

Podéis descargaros esta Live-CD de la siguiente dirección:

http://img259.imageshack.us/img259/8307/wifiway1zc4.jpg

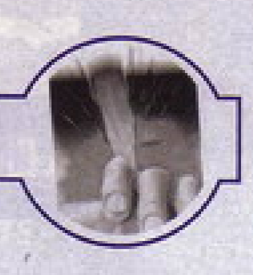
Live-CD desarrollada en España. Podéis conseguir información muy útil de su funcionamiento como información de interés general en; http://www.seguridadwireless.net/

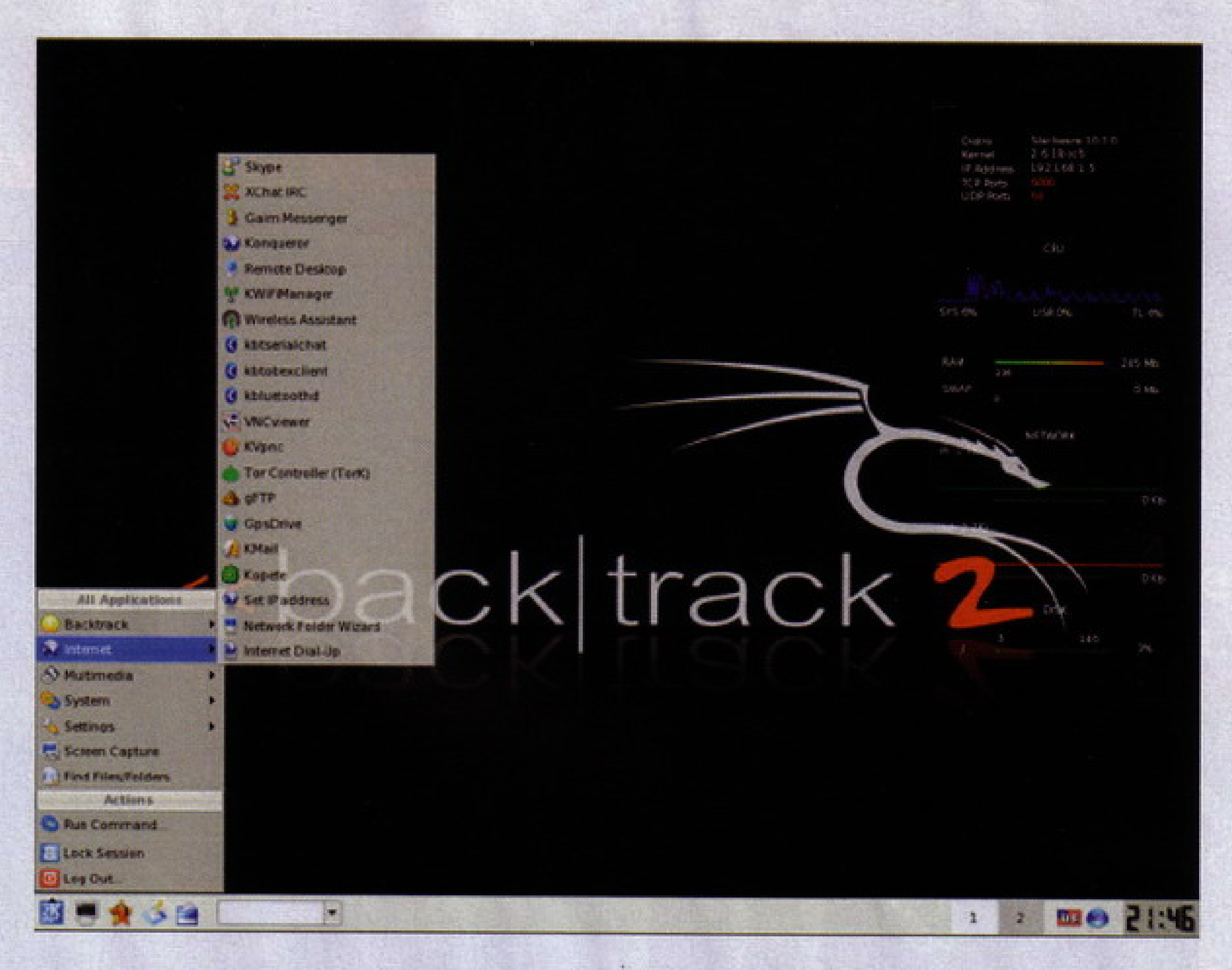
Wifislax

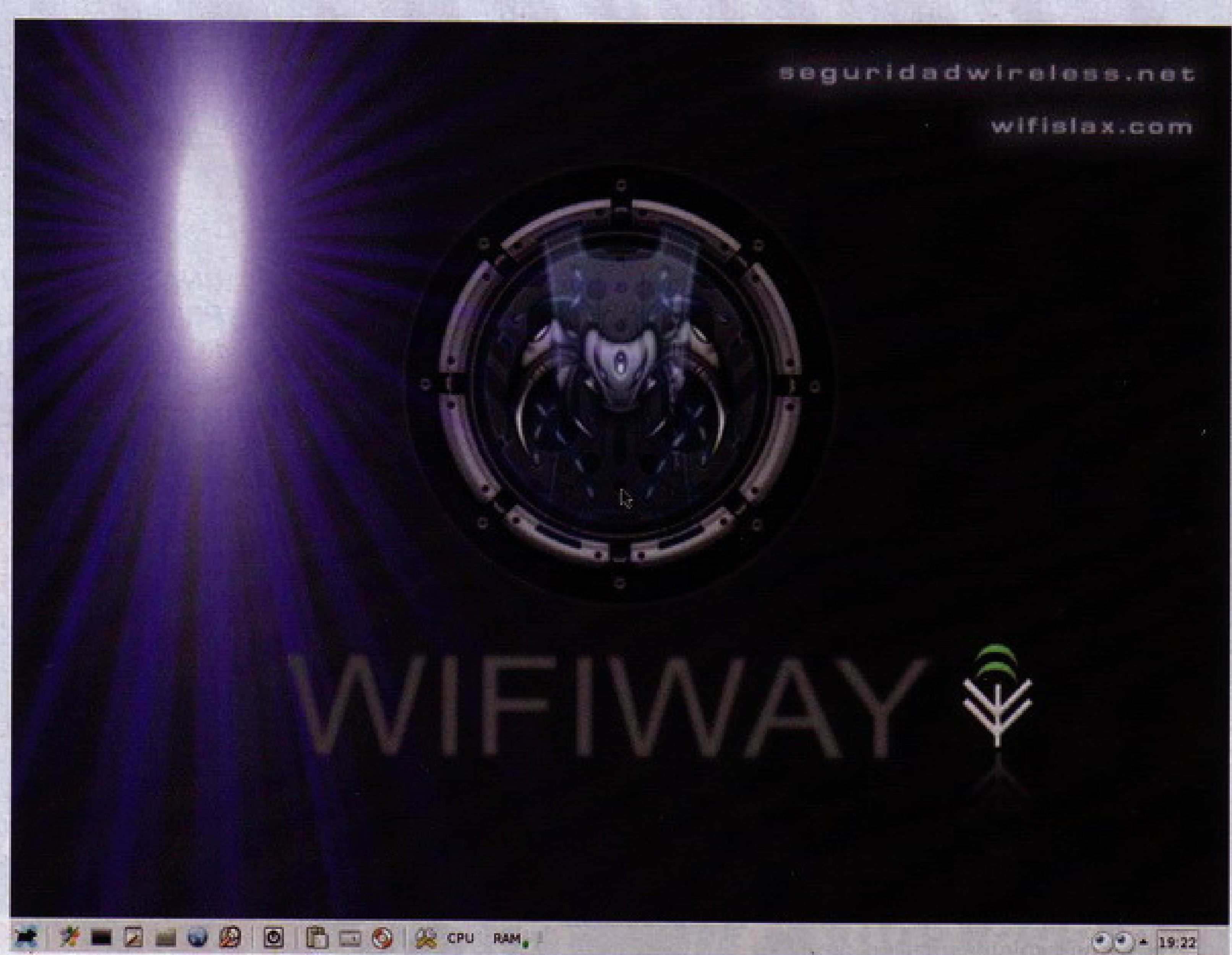
Podéis descargaros esta Live-CD de la siguiente dirección:

http://download.wifislax.com/wifislax-3.1.iso

Más información en: http://www.wi-




Skype
XChat IRC
Gaim Messenger
Konqueror
Remote Desktop
KWiFiManager
Wireless Assistant
kbtserialchat
kbtobexclient
kbluetoothd
VNCviewer
KVpnc
Tor Controller (TorK)
gFTP
GpsDrive
KMail
Kopete
Set IP address
Network Folder Wizard
Internet Dial-Up
All Applications
Backtrack
Internet
Multimedia
System
Settings
Screen Capture
Find Files/Folders
Actions
Run Command...
Lock Session
Log Out...
back|track 2
21:46


seguridadwireless.net
wifislax.com
WIFIWAY
CPU
RAM
19:22



fislax.com/

También disponéis de una versión más pequeña de unos 290 Megasbits

Podéis descargarla de la siguiente dirección:

http://foro.seguridadwireless.net/index.php/topic,5647.0.html

Troppix 1.2

Podéis descargaros esta Live-CD de la siguiente dirección:

http://distrowatch.com/table.php?distribution=troppix

También podéis ir probando por vuestra cuenta muchas de las Live-CDs que se exponen en:

http://www.distrowatch.com/
http://dir.linuxforums.org/
http://iso.linuxquestions.org/troppix/
http://www.madtux.org/

Podéis conseguir información alternativa en mi blog, que por cierto, cuenta que un nuevo dominio: http://blog.netting.es

Por último, comentaros que en cuanto pueda desarrollaré un portal en http://www.netting.es sobre seguridad informática. Una de las ideas principales es crear un foro en phpBB (http://foro.netting.es) para que los usuarios de la revista @rroba podáis preguntar cualquier duda que tengáis acerca de los artículos publicados.

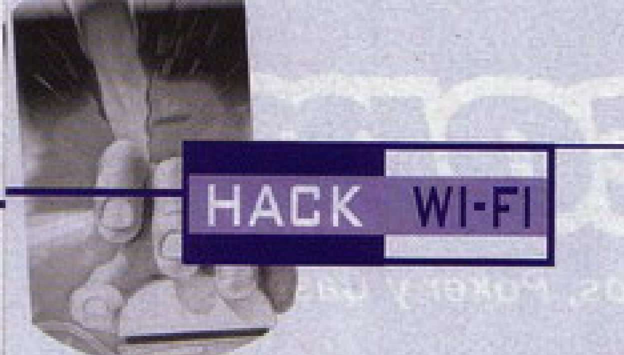
Sin más preámbulos entramos en materia.

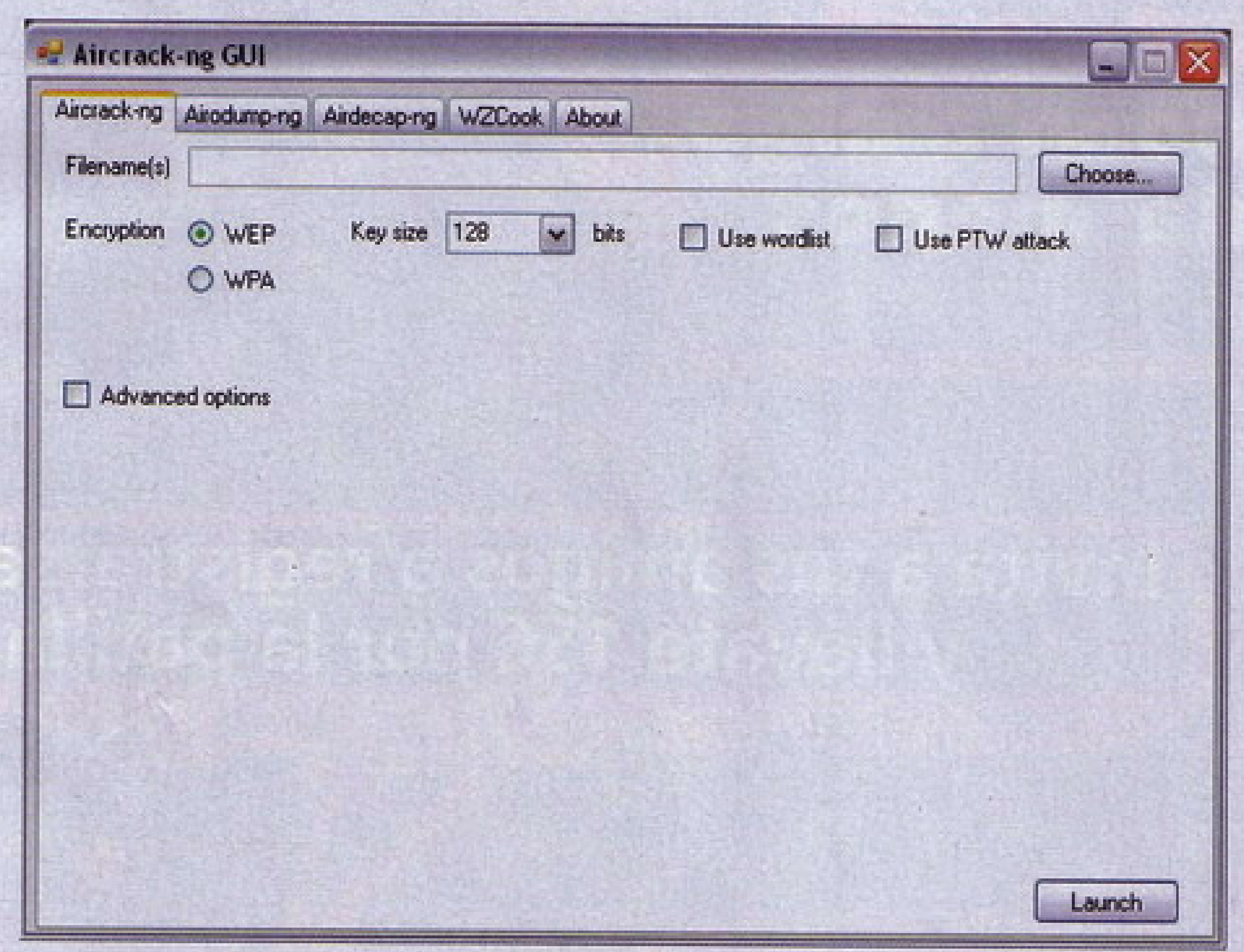
Seguimos donde lo dejáramos

En el artículo del mes anterior empezamos a estudiar la inyección de tráfico inalámbrico para el protocolo de cifrado WEP.

En este artículo, continuaremos con la teoría y empezaremos a hablar ya de algunos ataques que podemos realizar con la suite aircrack.

UNA DE LAS IDEAS PRINCIPALES ES CREAR UN FORO EN PHPBB (HTTP://FORO.NETTING.ES) PARA QUE LOS USUARIOS DE LA REVISTA @ RROBA PODÁIS PREGUNTAR CUALQUIER DUDA





PARA REALIZAR ESTOS ATAQUES DE INYECCIÓN INALÁMBRICA NO ES NECESARIO CONOCER TODA LA CLAVE WEP

Más teoría de inyección de tráfico cifrado del protocolo WEP

Esta vez centraremos la teoría en la inyección de tráfico inalámbrico en las capas más altas del modelo OSI.

Cuando realizamos un ataque de inyección de tráfico inalámbrico lo que estamos realizando, resumidamente, es duplicar paquetes predecibles de la red inalámbrica objetivo. Aunque esta no es la única forma disponible de para introducir datos cifrados en la red inalámbrica a atacar.

Para realizar estos ataques de inyección inalámbrica no es necesario conocer toda la clave WEP. Nos llega con conocer una parte de la cadena de la clave para un vector de iniciación (IV) específico, todo ello para poder inyectar datos válidos.

¿Cómo podemos conocer una parte de la cadena de la clave (seudoaleatoria)?

Si conocemos el texto plano y el texto cifrado correspondiente podemos combinarlos mediante la operación XOR para conseguir parte de esta cadena.

Las cabeceras de los paquetes, que deben ser conformes con a los estándares del protocolo, son una fuente aún ideal para conseguir datos conocidos en texto plano. Sin embargo, la autentificación mediante clave compartida basada en el protocolo de cifrado WEP de las redes inalámbricas (IEEE 802.11) ofrece una fuente aún mejor para conseguir parejas de datos como texto plano y texto cifrado. Se basa en el envío de una cadena en texto plano de uso único, conocido como nonce, a la máquina que trata de autentificarse. Esa palabra de uno único, el nonce, se cifra mediante la clave WEP y se envía de vuelta al punto de acceso, que comprueba si realmente la clave es correcta. De este modo, si se captura el nonce tanto como texto plano como en su forma cifrada, así como el vector de iniciación (IV) como texto plano, un atacante podría tener una oportunidad maravillosa para obtener una parte válida de la cadena de la clave.

Este tipo de ataques que hemos estudiado hasta hora son totalmente pasivos y confían en que haya tráfico cifrado en la red inalámbrica.

¿Pero, es posible inyectar tráfico en una red inalámbrica en la que no exista tráfico inalámbrico? La respuesta es totalmente afirmativa. Existen herramientas para reducir considerablemente el tiempo de ruptura del protocolo de cifrado WEP.

Es posible que introduzcamos nosotros mismo tráfico inalámbrico.

Pasemos ahora a la práctica y comprobemos como es posible, mediante la suite aircrack, romper una clave WEP de



una red inalámbrica objetivo inyectando paquetes, con y sin cliente asociados a la red inalámbrica.

La suite Aircrack.

Aircrack es una suite de herramientas para la auditoria inalámbrica. Con aircrack podemos comprobar la seguridad de nuestra red inalámbrica.

Resumidamente, aircrack es un detector de redes inalámbricas, un analizador de paquetes, un crackeador de sistemas de cifrado de las redes inalámbricas, un inyector de paquetes, etc...

Funciona con cualquier tarjeta inalámbrica que soporte el modo MONITOR / RFMON y pueda inyectar paquetes. Puede sniffar paquetes de varios estándares: IEEE 802.11a, IEEE 802.11b, IEEE 802.11g.

Y por encima es soportado por varios sistemas operativos: MS Windows y GNU/LiNUX.

En abril de 2007 un equipo de la Universidad Tecnológica de Darmstadt, en Alemania desarrolló un nuevo método de ataque basado en un documento publicado en el RC4 cifrado por Adi Shamir.

Este nuevo ataque, llamado "PTW", disminuye la cantidad de vectores de inicialización o IVs necesarios para descifrar la clave WEP y se ha incluido en el aircrack ng - Suite desde la versión 0.9.

Aircrack - ng es una bifurcación del proyecto original de Aircrack.

A la hora de escribir este artículo se encuentra disponible la versión aircrack-ng 0.9.1 (25 de Junio de 2007)

Podéis descargar aircrack-ng de los siguientes direcciones:

GNU/LiNUX:
http://download.aircrack-ng.org/aircrack-ng-0.9.1.tar.gz

MS Windows:
http://download.aircrack-ng.org/aircrack-ng-0.9.1-win.zip

Os recomiendo encarecidamente visitar la página del proyecto. Está muy documentada y seguro que nos echa una mano si tenemos algún problema:

http://www.aircrack-ng.org/

Como observáis aircrack nos brinda muchas posibilidades y no se limita a ser un crackeador de sistemas de cifrado inalámbrico, como piensan algunos.

Muchos usuarios novatos e inexpertos caen en el error de pensar que aircrack es un simple crackeador de ruptura del protocolo de cifrado WEP. Nada más lejos de la realidad.

Este error se debe a que la herramienta aircrack, que da nombre a la suite de



herramientas, es el crackeador de sistemas de cifrado inalámbrico.

Pasemos a instalar aircrack en nuestro sistema operativo inalámbrico.

Aircrack-ng en MS Windows

Instalar aircrack-ng en MS Windows no tiene ninguna dificultad Nos vasta con descargar el fichero comprimido de http://download.aircrack-ng.org/aircrack-ng-0.9.1-win.zip y descomprimirlo en una carpeta.

La mayor dificultad a la hora de utilizar esta herramienta es que nuestra tarjeta inalámbrica sepa trabajar con la suite aircrack.

En Microsoft Windows disponemos de una interesante interfaz gráfica para facilitarnos muchos procesos. La interfaz es muy intuitiva. De todas maneras, recordar que siempre se tiene un mayor control total de una herramienta utilizando la consola de comandos, nuestra querida y amiga consola negra, shell o como quieras llamarle ;)

Más adelante, en otro artículo de Hack Wi-Fi, nos centraremos en este sistema operativo. Mientras tanto haz pruebas tu mismo con esta suite de herramientas.

Aircrack-ng en GNU/LiNUX

Instalar aircrack-ng en GNU/LiNUX es también bastante sencillo.

Podemos bajarnos el código fuente y más material interesante como parches, de:

http://download.aircrack-ng.org/aircrack-ng-0.9.1.tar.gz

Y compilarlo a mano.

También podemos tirar de apt-get install :b

Desde Ubutu, lanzamos apt-get install desde un Terminal:

```
apt-get update

apt.get install aircack-ng
```

Si tenemos algún problema de librerías, las instalamos en el sistema del mismo modo.

Primero tirar de http://packages.ubuntu.com, para comprobar si está disponible la librería, como se llama y obtener más información al respecto.

```
Apt-get install libreria
```

Como ya comentábamos, lo que mayor problema nos puede ocasionar al utilizar la suite aircrack es que las tarjetas inalámbricas soporten el modo MONITOR / RFMON y puedan inyectar paquetes.

Por eso, a modo de ejemplo, os pongo aquí como instalar los controladores y parchear el controlador de varias tarjetas inalámbricas más conocidas y más famosas.

Si tu tarjeta inalámbrica no aparece aquí, tienes varias posibilidades:

a) Tirar del amigo Google para sacar información.

b) Pasarte por Wadalbertia.org y postear tus problemas.

c) Pasarte por http://foro.netting.es y postear tus problemas. Espero que para cuando sea publicado este artículo el foro esté 100% operativo.

Chipset Atheros (PCI / PCMCIA):

Para mi tarjeta inalámbrica D-Link G520.

```
    ifconfig ath0 down
    ifconfig wifi0 down
    rmmod wlan_wep ath_
rate_sample ath_rate_onoe
\ ath_pci wlan ath_hal ath_
rate_amrr 2>/dev/null
    wget http://snapshots.
madwifi.org/madwifi-ng-
current.tar.gz
    wget http://patches.
aircrack-ng.org/madwifi-
ng-r2277.patch
```

En http://patches.aircrack-ng.org podréis comprobar cuales son los parches más actuales.

Desempaquetamos y descomprimimos el fichero que nos hemos descargado con wget:

```
    tar -zxvf madwifi-ng-
current.tar.gz
```

Navegamos hasta el directorio donde se encuentran los ficheros descomprimidos:

```
    Cd madwifi-ng
```

Y lanzamos los parámetros necesarios:

```
    patch -Np1 -i ../madwifi-
ng-r2277.patch
```

LA MAYOR DIFICULTAD A LA HORA DE UTILIZAR ESTA HERRAMIENTA EN WINDOWS ES QUE NUESTRA TARJETA INALÁMBRICA SEPA TRABAJAR CON LA SUITE AIRCRACK



```
make

make install

depmod -ae

modprobe ath_pci
```

Aquí os pongo los parámetros que debemos de utilizar para poner la tarjeta inalámbrica con el controlador Madwifi en varios estados a través de wlanconfig:

```
$ wlanconfig

Usage: wlanconfig athX create [nounit] wlandev wifiY wlanmode [sta | adhoc | ap | monitor | wds | ahdemo] bssid | -bssid] [nosbeacom]

Usage: wlancofig athX destroy

Usage: wlanconfig athX list [active | ap | caps | chan | freq | keys | scan | sta | wme]
```

Antes de poner la interfaz en algún estado debemos de destrozar la interfaz con:

```
$ wlanconfig athX destroy
```

Siendo X el número que utilizamos para la interfaz, por ejemplo: ath0, ath1...

Para poner la tarjeta inalámbrica en algún estado utilizamos:

```
$ wlanconfig athX create wlandev wifiY wlanmode aqui_el_estado
```

Siendo X e Y números que utilizaremos para identificar la interfaz. Las tarjetas inalámbricas con chipset Atheros y con el controlador Madwifi soportan varios estados: ad-hoc (estado que todavía no nos hemos centrado en el aunque si hemos estudiado como funciona), monitor (para capturar paquetes), manager (para trabajar de forma normal con la tarjeta inlaámbrica), ap (para que la tarjeta inalámbrica trabaje en modo de infraestructura, estado que ya hemos estudiado), etc...

Al introducir estos parámetros se debe de mostrar en pantalla la interfaz creada, siempre y cuando la interfaz se haya creado correctamente.

Chipset RT2570 (USB):

```
ifconfig rausb0 down

rmmod rt2570

wget http://homepages.tu-darmstadt.de/~p_larbig/wlan/rt2570-k2wrlz-1.6.1.tar.bz2

tar -xvjf rt2570-k2wrlz-1.6.1.tar.bz2

cd rt2570-k2wrlz-1.6.1/Module

make && make install

modprobe rt2570
```

http://hwagm.elhacker.net/drivers-ng/driver-ng.htm

Chipset Ralink RT73 (USB)

```
ifconfig rausb0 down

rmmod rt73

wget http://homepages.tu-darmstadt.de/~p_larbig/wlan/rt73-k2wrlz-2.0.0.tar.bz2

tar -xjf rt73-k2wrlz-2.0.0.tar.bz2

cd rt73-k2wrlz-2.0.0/Module

make && make install
modprobe rt73
```

Para poner la tarjeta inalámbrica en modo MONNITOR / RFMON:

```
Iwconfig rausb0 mode monitor
```

```
Chipset Zydas (USB)
rmmod zd1211rw
```

Es recomendable librerar de la memoria lo siguiente:

```
rmmod ieee80211softmac

rmmod ieee80211
```

Al igual que cualquier rastro de ieee80211

```
wget http://patches.aircrack-ng.org/ieee80211_inject.patch
wget http://patches.aircrack-ng.org/zd1211rw_inject_2.6.22.patch

cp ./ieee80211_inject.patch /usr/src/linux

cp ./zd1211rw_inject_2.6.22.patch /usr/src/linux

patch -Np1  --verbose --dry-run -i zd1211rw_inject_2.6.22.patch

patch -Np1  --verbose  -i zd1211rw_inject_2.6.22.patch

patch -Np1  --verbose --dry-run -i ieee80211_inject.patch

patch -Np1  --verbose  -i ieee80211_inject.patch

cd /usr/src/linux/drivers/net/wireless/zd1211rw

make -C /lib/modules/`uname -r`/build/ M=`pwd` modules

make -C /lib/modules/`uname -r`/build/ M=`pwd` modules_install

cd /usr/src/linux/net/ieee80211

make -C /lib/modules/`uname -r`/build/ M=`pwd` modules

make -C /lib/modules/`uname -r`/build/ M=`pwd` modules_install

depmod -ae

modprobe zd1211rw
```

Es aconsejable reiniciar el sistema, exceptuando cuando utilizamos una Live-CD.

Chipset Ipw2200 (MiniPCI)

```
wget http://superb-west.dl.sourceforge.net/sourceforge/ieee80211/ieee80211-1.2.17.tar.gz

tar zxvf ieee80211-1.2.17.tar.gz

cd ieee80211-1.2.17

make

make install

wget http://telefonica.net/web2/wifislax/varios/ipw2200-1.2.1-inject_patch.tar.gz

wget http://superb-west.dl.sourceforge.net/sourceforge/ipw2200/ipw2200-1.2.1.tgz

tar zxvf ipw2200-1.2.1.tgz

tar zxvf ipw2200-1.2.1-inject_patch.tar.gz

patch ipw2200-1.2.1/ipw2200.c ipw2200-1.2.1-inject.patch

patch ipw2200-1.2.1/Makefile ipw2200-1.2.1-inject_Makefile.patch

cd ipw2200-1.2.1

./remove-old

make

make install

rmmod ipw2200

modprobe ipw2200 rtap_iface=1

HOSTAP - PCI / PCMCIA chipset prism 2 y 3
```

Los siguientes pasos son útiles en un kernel superior o igual al 2.6.16

```
cd /usr/src/linux

wget http://patches.aircrack-ng.org/hostap-kernel-2.6.18.patch

patch -Np1 --verbose --dry-run -i hostap-kernel-2.6.18.patch

patch -Np1 --verbose -i hostap-kernel-2.6.18.patch

cd /usr/src/linux/drivers/net/wireless/hostap

rm /lib/modules/`uname -r`/kernel/drivers/net/wireless/hostap/*

make -C /lib/modules/`uname -r`/build/ M=`pwd` modules

make -C /lib/modules/`uname -r`/build/ M=`pwd` modules_install

depmod -a

modprobe hostap_pci

Kernel inferior al 2.6.16
ifconfig wlan0 down

wlanctl-ng wlan0 lnxreq_ifstate ifstate=disable

/etc/init.d/CardBus stop

rmmod prism2_pci

rmmod hostap_pci

wget http://hostap.epitest.fi/releases/hostap-driver-0.4.9.tar.gz

tar -xvzf hostap-driver-0.4.9.tar.gz

cd hostap-driver-0.4.9

wget http://patches.aircrack-ng.org/hostap-driver-0.4.7.patch

patch -Np1 -i hostap-driver-0.4.7.patch

make && make install

mv -f /etc/pcmcia/wlan-ng.conf /etc/pcmcia/wlan-ng.conf~
/etc/init.d/pcmcia start

modprobe hostap_pci &>/dev/null
```

Conclusiones

Este mes tenía pensado empezar ya a explicar los diferentes ataques que podemos realizar con aircrack-ng, sus herramientas, etc.

Antes de meternos de lleno en esto, es necesario que nuestras tarjetas inalámbricas se adapten perfectamente al sistema operativo y sepan trabajar con el, de lo contrario, no podremos realizar las prácticas con éxito. Y, como siempre digo, las prácticas nos ayudan muchísimo a entender el funcionamiento de las mismas. Así que mejor preparemos todo perfectamente.

Si tenéis algún problema con vuestra tarjeta inalámbrica ya sabéis que tenéis que hacer, espero que para cuando se publique este artículo ya esté el foro phpBB totalmente operativo, http://foro.netting.es.

En este artículo hemos tocado ya la última porción de teoría sobre inyección de tráfico inalámbrico para la ruptura del protocolo de cifrado WEP. Quizás más adelante toquemos otro poquito de teoría, pero toda ella acompañado con su respectiva práctica, para aclarar mejor las cosas.

En el próximo número.

En el próximo capítulo de Hack W-Fi seguiremos estudiando el protocolo de cifrado WEP y como inyectar tráfico inalámbrico cifrado. Espero que para el próximo capítulo empecemos ya con un poco de práctica, por eso de no aburrirnos mucho con tanta teoría e instalación de controladores, etc.

Como no tengo muy claro todavía lo que vamos a tocar en el próximo capítulo estar atentos a mi blog. También, quizás, os interese pasaros por http://www.netting.es para estar más actualizados con noticias sobre seguridad informática.

Un saludo lectores ;)

NeTTinG (Enrique Andrade González)
nettinghxc@gmail.com
http://www.wadalbertia.org
http://www.foro.netting.es
http://blog.netting.es



MUSICA ORIGINAL
CONVIERTE TU MOVILE EN UN MP3 PORTATIL
sms envía MUSICA19 (espacio) código de cancion al 7494
Rechaza imitaciones
EJEMPLO: para descargarte LA SINTONIA de los SIMPSOS tienes que enviar MUSICA19 26189 al 7494
25017 UMBRELLA
7312 HIMNO OFICIAL DEL CENTENARIO DEL SEVILLA F.C.
0358 ATREVETE-TE
25569 LAMENTO BOLIVIANO (XTM RMX) Dani Mata
17644 AMOR GITANO (BSO EL ZORRO) Alejandro Fernandez
28376 YOUNG FOLKS Peter Bjorn & John
13725 LAS DE LA INTUICION Shakira
27825 FAR FROM HOME (ORIGINAL SPOT) Tiga
28362 ME ENAMORA Juanes
27654 RELAX Mika
13552 QUE HICISTE Jennifer López
26133 ME GUSTA EL FÚTBOL Melendi
25394 COMO LA VIDA (VUELTA CICLISTA 07) Hanna
27415 1973 James Blunt
28757 LA DOLCE VITA Soraya
14244 ALL GOOD THINGS Nelly Furtado
17452 ADOLESCENTES
3679 EL PADRINO
14600 ECUADOR
26126 ÁFRICA
17697 CALL ME
13567 HOW TO SAVE A LIFE (BSO ANATOMIA DE GREY)
29509 TODO IRA BIEN
9696 EN LA PLANTA DE TUS PIES
27504 THE SIMPSONS THEME
1486 ME MUERO
17420 MONSOON
13884 MICROMANIA
1593 TU RECUERDO
27692 APROXIMACIÓN
29735 POR TÍ DARÍA
28648 DO IT WELL
13744 QUIERO QUE SEPAS
29615 GIMME MORE
17798 DO YOU KNOW (THE PING PONG SONG)
25129 HOT SUMMER NIGHT (OH LA LA LA)
1488 SUEÑOS ROTOS
6701 HIGHWAY TO HELL
28498 TODO SE PARECE A TI
77224 BSO EL BUENO, EL FEO Y EL MALO
26122 ACABO DE LLEGAR
7186 BSO LA PANTERA ROSA Cine y televisión
28403 MIRA LO QUE TE HAS PERDIDO
0654 HIMNO OFICIAL DEL CENTENARIO DEL BETIS
13235 VUELVETE A LA LUNA
14609 PARA TODA LA VIDA
4883 TORRE DE BABEL (REGGAETON MIX)
14358 MORENAMIA (DUETO 2007)
3680 EYE OF THE TIGER (BSO ROCKY III)
26189 BSO LOS SIMPSONS Cine y televisión
25395 DÉJAME VIVIR Jarabe de Palo
2340 MAIN TITLE (BSO EL ULTIMO MOHICANO)
25581 MY OWN WAY
27812 LA ACEITUNA
17591 SER O PARECER RBD Rebelde
9030 NI UNA SOLA PALABRA Paulina Rubio
9908 COMO EN UN MAR ETERNO
17792 KILLING IN THE NAME (LIVE)
9150 PARA QUE TU NO LLORES
13588 QUIEREME Andy y Lucas
Harry Potter
CINE Y TELEVISIÓN
POLIFONICOS
ÚSALOS COMO TONOS DE LLAMADA PARA TUS AMIGOS
sms envía TONOS4 (espacio) código polifonico al 7494
EJEMPLO: para descargarte "BSO DEL ZORRO" tienes que enviar TONOS4 92061 al 7494
bájate todos los éxitos ¡¡¡para tu móvil!!!
92272 Umbrella
89601 Himno O. Del Cent. Del Sevilla F.C.
82172 Barcelona
91207 Atrevete-te
84724 BSO El bueno, el feo y el malo
92061 Amor gitano (BSO El Zorro)
90804 Tu Recuerdo
85220 Himno de la legión
83188 Real Madrid
83227 Salve Rociera
84207 El Padrino
82984 Paquito El Chocolatero
91504 Las de la intuicion
92747 Young folks
80082 BSO La pantera Rosa
85529 BSO El ultimo mohicano
83808 Himno de España
90385 Torre de Babel (Db Original Mix)
84362 Champions League
84966 24 - Serie TV
85333 You´ll never walk alone
82123 Athletic De Bilbao
84560 Sintonía Curro Jimenez
82124 Atletico De Madrid
92665 Me enamora
84067 El Exorcista (Tubular bells)
84489 Els segadors
84494 La internacional
82873 Muñeira De Chantada
84490 Asturias patria querida
92551 Lamento boliviano
84446 Cara al sol
85607 Sintonía El pajaro loco
84094 Himno de riego
83883 Sintonía cabecera Fraggle Rock
92634 Far from home (Original spot)
80017 BSO Mision imposible
80039 Eye of the tiger (BSO Rocky III)
92011 Adolescentes
90623 Himno oficial del centenario del Betis
85606 Vals de Amelie
92503 Ecuador
91412 Que hiciste
84437 Sintonía Shin Chan
83326 Soy Minero
80108 Sintónia Benny Hill
83737 Dragon Ball Z
83648 Sintonía La familia Monster
84202 Telefono antiguo
84064 Darth Vader Marcha imperial
92612 Relax
84999 Sintonía cabecera CSI Miami
ATENCIÓN AL CLIENTE 902 01 30 16 (10 - 19 horas)
LOGOS Y TONOS
www.LOGOSYTONOS.com
JUEGOS
Descárgatelos al móvil y juega donde y cuando quieras
sms envía JUEGOS30 (espacio) código juego al 7494
EJEMPLO: para descargarte "BISBAL FAN FACTOR" tienes que enviar JUEGOS30 3094 al 7494
convierte tu móvil en una consola de juegos
David Bisbal FAN Factor
código 3094
MOBILE BODY TRAINER
entrenador personal físico
código 3098
SHREK TERCERO
código 3091
código 3092
código 1836
MIAMI NIGHTS
código 3035
¡ALLA TU!
DOGZ
código 3089
¡Entrena tu mente y conviértete en el más listo de tus amigos!
SONIC JUMP
código 3025
BRAIN CHALLENGE
código 2616
código 3107
REAL FOOTBALL 2007
código 1435
TOP JUEGOS
2034 ZUMA
3093 MOBI LOVER
1181 CONECTA 4
7741 SONIC THE HEDGEHOG
1051 BUBBLE BASH
3024 DESEOS OCULTOS
2611 BOCA SECA MAN
5577 VIRTUA TENNIS MOBILE
9585 SEXY VEGAS ANASTASIA MAYO
1459 SEXY SHANGAI
258 DOMINO FEVER
2613 MUJERES DESESPERADAS
3085 FLEXIS
1457 Prince of Persia - Las 2 coronas
TEMAS
TEMA = FONDO + ICONOS
sms envía MENU26 (espacio) código del tema al 7494
FONDO + ICONOS
Perros código 14584
Fantasmas código 0165
Horoscopo código 14449
Culturistas código 13789
¡llénalo de coches tuneados!
Tuning World código 1582
SONIBROMAS
sms envía POLITONO83 (espacio) código polifonico al 7808
ÚSALOS COMO TONOS DE LLAMADA PARA TUS AMIGOS
77435 Osea te cojo el telefono
77395 Mensaje del caudillo
77762 Como el luisma no se entera
77642 El teléfono es mi tesoro
26735 Coge el maldito teléfono
78862 Sevilla - Hasta la muerte
78854 R. Madrid - Fieles y leales
77148 La guardia civil
1583 Tikitaka
27457 Padre nuestro pijo
79386 F1 Alonso
78851 Barça - La la la Fc Barcelona
7277 Bernardo Camera Cafe Mari Carmen
78868 R.Madrid - Coge el móvil
79094 Atleti, Atleti, Atlético de Madrid
26729 Dos cosas
6924 Cariño me lo puedes coger
79097 athleeeeeeeeeetic!
9670 Alcohol
XMESSENGER ahora para móviles
TUS CONTACTOS SIEMPRE CONTIGO
sms envía MSX46 (espacio) 2269 al 7494
MESSENGER EN TU MÓVIL
PRECIO SMS: 1,2 €/MEN +IVA; FROGGIE S.L. - CIF: B91109454. SÓLO MAYORES 18 AÑOS; APD.CORREOS 6079 - 41009 SEVILLA.



Los peligros del cross-site scripting

Bienvenidos a un número más de esta revista. En este artículo se hablará sobre una vulnerabilidad más que conocida, el Cross-Site Scripting (XSS), se hablará también del uso que se le está dando actualmente. Porque aunque no lo parezca puede llegar a tener gran importancia, de hecho, si se aprovecha correctamente puede llegar a ser bastante peligroso y perjudicial para el usuario.

Antes de empezar hay que decir que este error se basa principalmente en la ingenuidad de la víctima, así como la facilidad que tienen los usuarios de "aceptar" cada mensaje que proviene del navegador sin leerlo siquiera. Aunque también es posible realizar el ataque XSS sin que el cliente intervenga directamente, es decir, de manera invisible. Así que para empezar a introducir el tema se va a hablar de la herramienta predominante en los clientes de Internet, el navegador web.

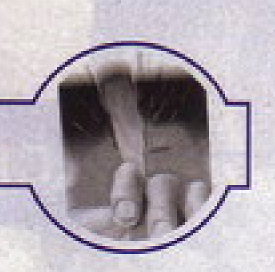
EL NAVEGADOR

Técnicamente, el navegador que se usa para visitar las páginas web, no es más que un intérprete de código que se comunica con un servidor. Como todo software ha ido evolucionando hasta tal punto que algo que era un simple navegador que permitía ver webs HTML y punto, ahora tiene otras mil funcionalidades.

Para el tema que importa ahora, XSS; se debe hablar de la interacción que se puede llevar a cabo desde el navegador. Según el site que se esta visitando, se dispone de un tipo de interacción u otro, dependiendo de la tecnología web usada. Por ejemplo, una web estática sólo proporciona información, y un usuario no podrá realizar muchas más acciones que pulsar en un link directo, ya que todo ocurre en el propio navegador, en cambió en una web dinámica se puede interaccionar con el servidor de una manera mucho más directa, por ejemplo, realizando peticiones con parámetros.

SEGÚN EL SITE QUE SE ESTA VISITANDO, SE DISPONE DE UN TIPO DE INTERACCIÓN U OTRO, DEPENDIENDO DE LA TECNOLOGÍA WEB USADA

Un pequeño listado de las tecnologías más "típicas" que soportan los navegadores actuales podrían ser: HTML, JavaScript, CSS... Cada una tiene su propia funcionalidad, además es posible añadir soporte para otro tipo de elementos, como Flash o Java, utilizando para ello plugins externos. Para poder ver la totalidad de tecnologías soportadas por los navegadores más usados, como Firefox e Internet Explorer, basta con acceder a http://developer.mozilla.org/ y http://www.microsoft.com/win-



dows/ie/ie6/evaluation/features/default.mspx respectivamente.

Como ya se ha dicho, cada uno de estas tecnologías web tiene su propia funcionalidad. Algunas simplemente se emplean para controlar el diseño y maquetación de la página web, para darle forma y color, HTML y CSS, e incluso JavaScript para añadir dinamismo. Otros, en cambio, pueden llegar a ejecutar código en la máquina del cliente pidiendo, evidentemente, permiso expreso, aunque no son pocos los casos en los que el usuario acepta sin tan siquiera leer los avisos emitidos por el navegador o por fruto de un engaño o despiste.

Con todo esto se quiere decir que el navegador puede realizar muchas funciones, algunas de las cuales pueden llegar a comprometer nuestra seguridad si se usan con malas intenciones. Algunos recordareis esos dialers de las páginas para adultos que se instalaban solos sin conocimiento del usuario. Es por eso que hay que dedicar especial atención a los mensajes procedentes de las visitas por Internet y aceptar solamente aquellos de los que se esté realmente seguro y provengan de una fuente de confianza.

LA INYECCIÓN

El concepto de inyección no solo se utiliza para referirse a un ataque de tipo XSS, de hecho se denomina inyección de caracteres arbitrarios, ya sea para producir un XSS (Inyección de código interpretada por un cliente Web, generalmente HTML o Javascript) o un SQL Injection (Inyección SQL interpretable por el servidor de la base de datos), se produce cuando las entradas de los parámetros en un CGI (scripts/programas que se encargan de generar la web) no están bien verificados. Consecuentemente, durante su ejecución en el momento de utilizar el valor del parámetro, se produce la inyección de todos los caracteres sin ningún tipo de validación, entonces es cuando se produce una inyección de código interpretable por el navegador/servidor dependiendo del caso.

EL CONCEPTO DE INYECCIÓN NO SOLO SE UTILIZA PARA REFERIRSE A UN ATAQUE DE TIPO XSS, DE HECHO SE DENOMINA INYECCIÓN DE CARACTERES ARBITRARIOS

Según la inyección, el problema es más o menos serio, en este artículo se hablará de la inyección de código HTML y Javascript, ya que son lenguajes que afectan directamente al cliente. También se podría hablar de inyecciones en el servidor, pero entonces sería otro tipo de problema: SQL Injection, PHP Injection, IMAP/SMTP Injection, LDAP Injection, SSI Injection... Y sería una explicación demasiado extensa.

El XSS no es más que una inyección HTML o Javascript, como ya se ha dicho anteriormente. Veamos un simple código a modo de ejemplo, meramente conceptual y que no funciona:

```
xss.cgi:
1: <HTML>
2:        <BODY>
3:        <?      print
$GET['var1']; ?>
4:</BODY>
5: </HTML>
```

Supongamos que la sentencia en la tercera línea se encarga de imprimir por pantalla el valor de la variable "var1" pasada por GET. Si se hiciera la siguiente llamada:

Servidor del Atacante

(1) Nueva Orden

¿Hay nueva orden? (2)

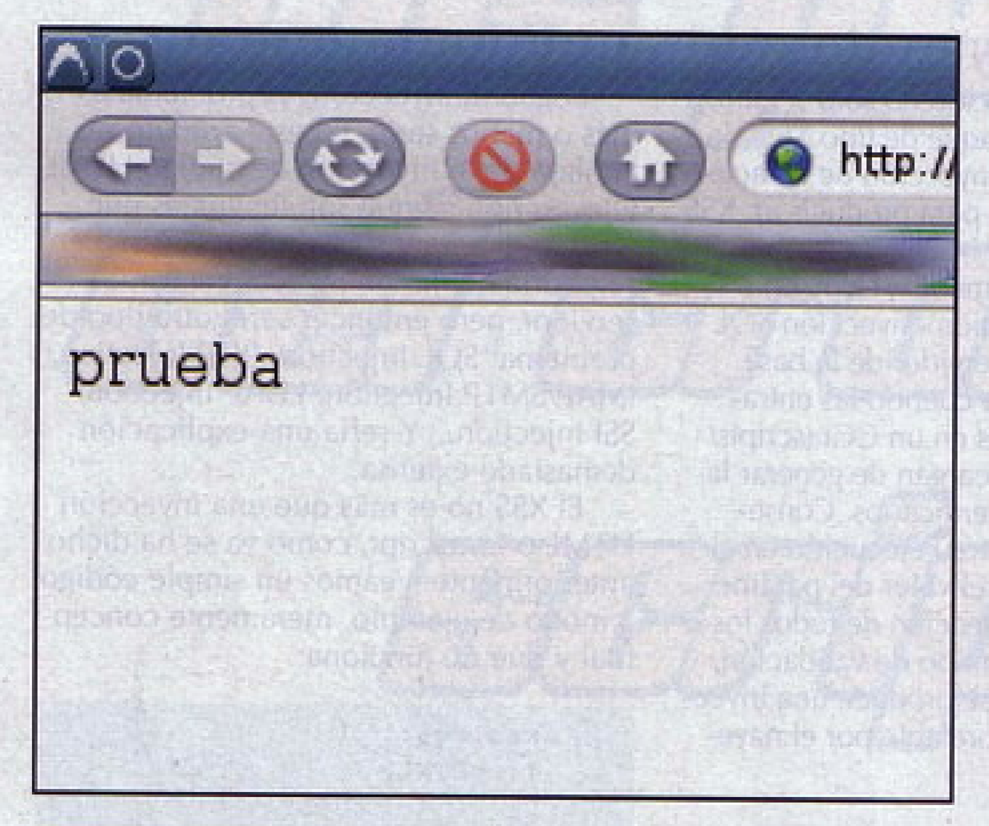
Nueva Orden (3)

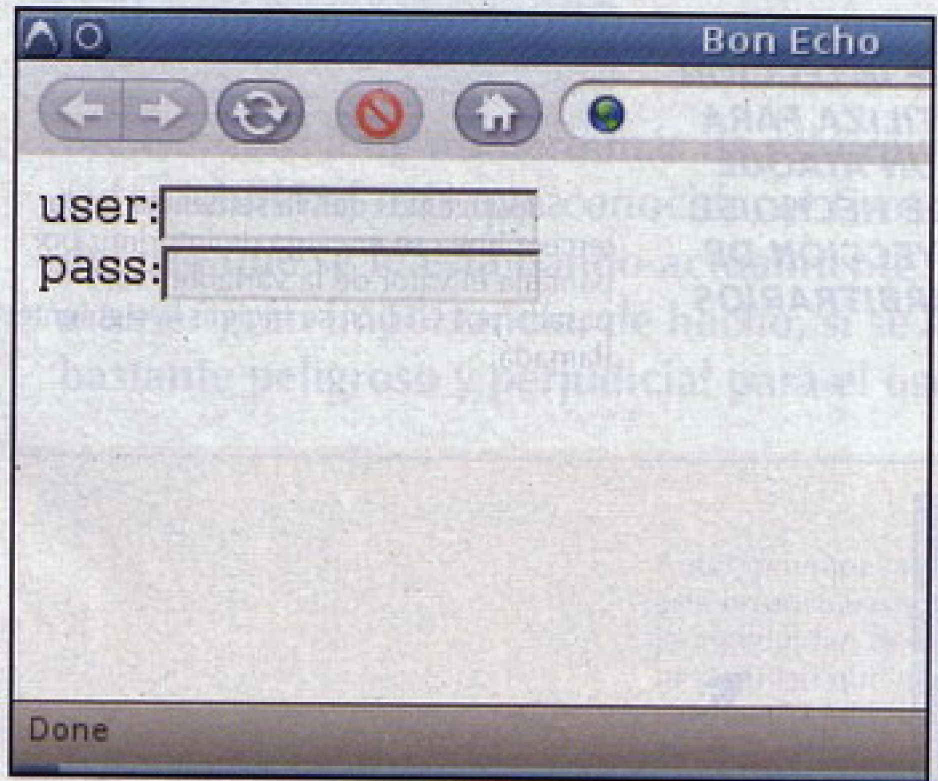
Atacante

Víctima

Funcionamiento de XSS Shell







DESTACAN LOS ATAQUES DE PHISING QUE MUCHAS VECES SE APROVECHAN DE VULNERABILIDADES DE XSS EN LAS APLICACIONES WEB ALOJADAS SERVIDORES LÍCITOS PARA HACERSE PASAR POR ELLOS, ROBANDO ASÍ LOS CREDENCIALES DE LA VÍCTIMA

```
http://www.server.com/xss.cgi?var1=prueba
```

La respuesta sería una web en blanco con la palabra "prueba" escrita al inicio (ver imagen1). Nada peligroso por el momento. Veamos ahora otro tipo de comportamiento. Añadiendo etiquetas HTML al valor de la variable podemos modificar el código resultante. Por ejemplo, pasando la cadena: 'user:<input type="text" length="25" />
pass:<input type="pass" length="25" />' directamente, es decir, con la llamada:

```
http://www.server.com/xss.
cgi?var1=user:<input type="text" length="25"
/><br />pass:<input type="pass" length="25" />
```

El resultado será el que se puede observar en la imagen2. Se puede ver que la salida es muy distinta a la anterior 'una web en blanco con la palabra "prueba"'. En este caso lo que ha ocurrido es que el navegador ha interpretado los caracteres que hemos inyectado. Dicho de otra manera, es posible inyectar cualquier código interpretable por el navegador y hacer que este se comporte en consecuencia.

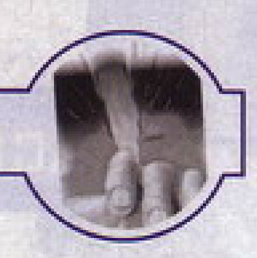
PHISING

Dependiendo de las motivaciones de quien realice la inyección se utilizará para un fin u otro. Principalmente destacan los ataques de phising que muchas veces se aprovechan de vulnerabilidades de XSS en las aplicaciones web alojadas servidores lícitos para hacerse pasar por ellos, robando así los credenciales de la víctima. Si se hiciera un ataque de este tipo a un banco, el atacante podría tener acceso total a las cuentas de la víctima. De hecho, cada día son más los casos de phising en todo el mundo, el correo SPAM que tanto se odia, muchas veces tiene ese objetivo, hacer creer realidades que no son, como por ejemplo tener que validar la contraseña de acceso al banco por algún problema técnico que ha tenido este.

Para realizar este ataque bastaría con imitar un formulario de login en la web vulnerable y enviar los datos a un servidor privado controlado por el atacante. Después, para infectar al usuario bastaría con postear el link o enviárselo por correo (spam). El esqueleto del código inyectado podría ser parecido al utilizado en el primer ejemplo y el resultado análogo al de la imagen2, sólo que con la estética de la web vulnerable que se pretenda suplantar.

MALWARE

Otra posible finalidad es la instalación de Malware en la máquina del cliente haciéndose pasar por el servidor de la entidad. Esto se podría conseguir añadiendo algunas líneas de código que fueran suficientes para que el navegador hiciera



una petición de descarga al servidor controlado por el atacante. El XSS entra en juego para camuflar al atacante. Al realizar la inyección del código necesario en la web original, crea al usuario la sensación de seguridad de que se esta descargando el programa del sitio correcto, ya que él está visitando esa web en ese instante.

Los programas descargados de esta manera pueden ser tanto un fichero que luego es necesario que el usuario lo ejecute confiando con el origen en una fuente de confianza, a modo de actualización por ejemplo, o bien un applet Java o ActiveX. Que se encargará de hacer todas las acciones necesarias para la infección. Así que hay que asegurarse siempre bien de dónde se están bajando los ficheros y validar la autoría del remitente.

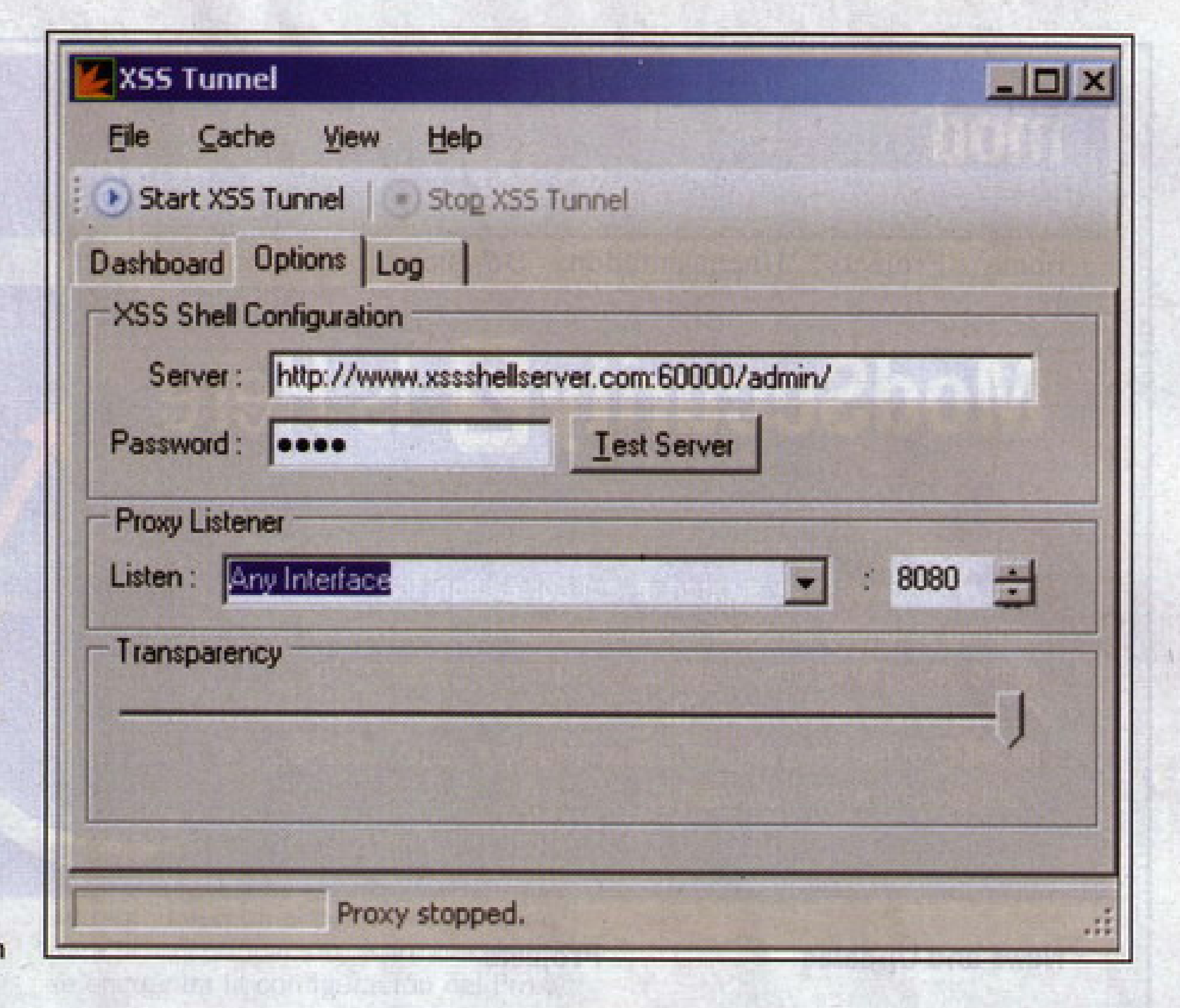
TÉCNICAS AVANZADAS

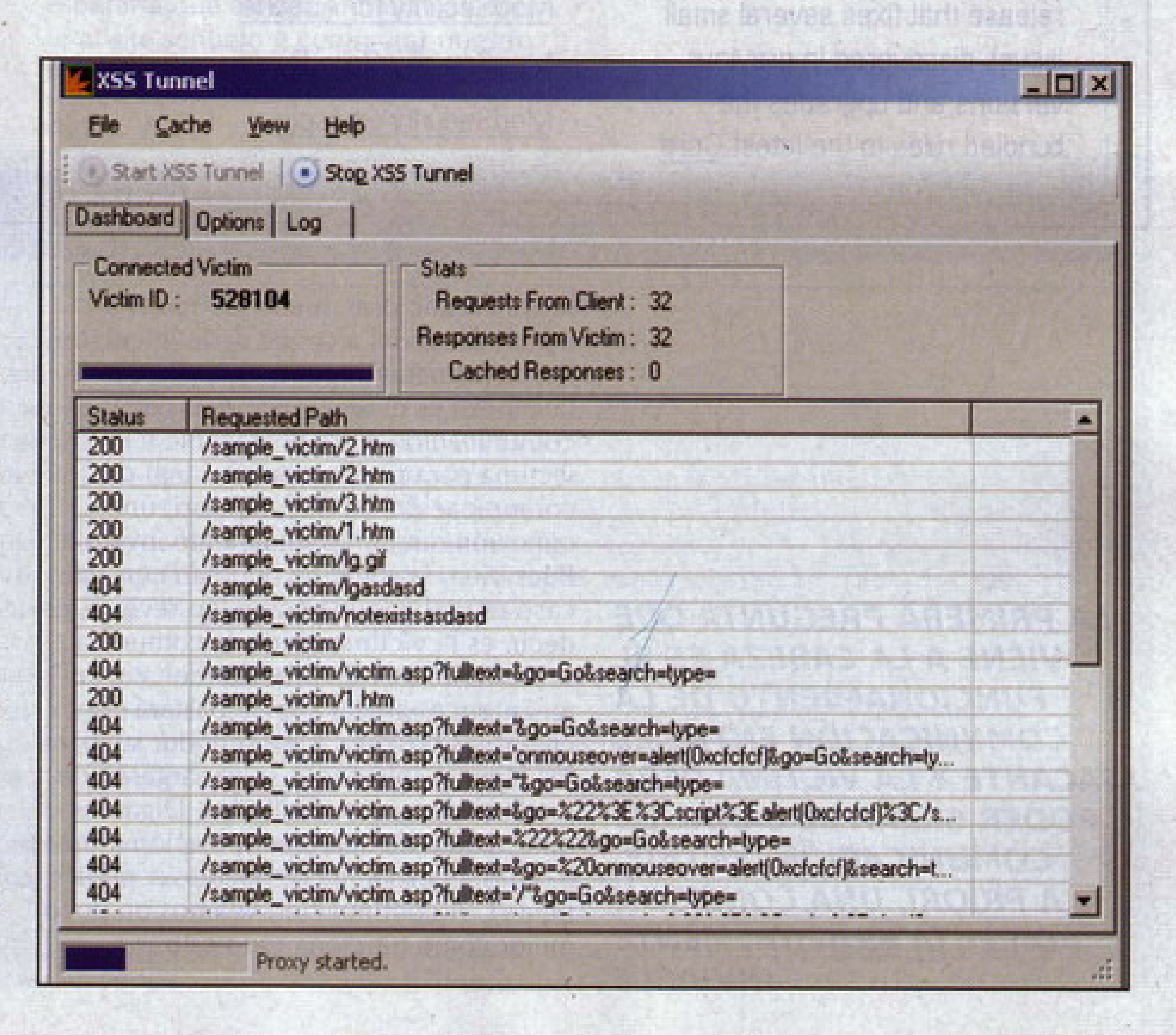
Lo visto hasta ahora es lo 'típico', pero también existen otras posibilidades de las que no se habla tanto, aunque tengan algún que otro año de vida. La compañía 'Portcullis Computer Security', en concreto Ferruh Mavituna, por ejemplo ha realizado unas aplicaciones realmente interesantes que aprovechan de manera óptima todo lo relacionado con el concepto de Cross-SiteScripting. Las herramientas en concreto se denominan XSS-Tunnel y XSS-Shell y pueden conseguirse en el siguiente enlace:

http://www.portcullis-security.com/16.php

En esta página se pueden observar todas las aplicaciones gratuitas que ofrecen, todas ellas bastante interesantes (ver imagen3).

El objetivo de XSS Shell es controlar el navegador de la víctima, mientras que XSS Tunnel llega un poco más allá y es capaz de crear un canal de comunicación entre el atacante y la red, pasando por la víctima o, lo que es lo mismo, un proxy. Ambas se sirven de la misma técnica, inyectar código javascript para infectar el navegador al mismo tiempo que regeneran la web vulnerable a ataques de tipo XSS. De esta manera se mantiene a la víctima en un entorno virtual controlado, aunque este echo supone alguna que otra restricción. Por ejemplo, si pensamos en los navegadores actuales con pestañas, en este caso solo se infectaría la pestaña que hubiera accedido a







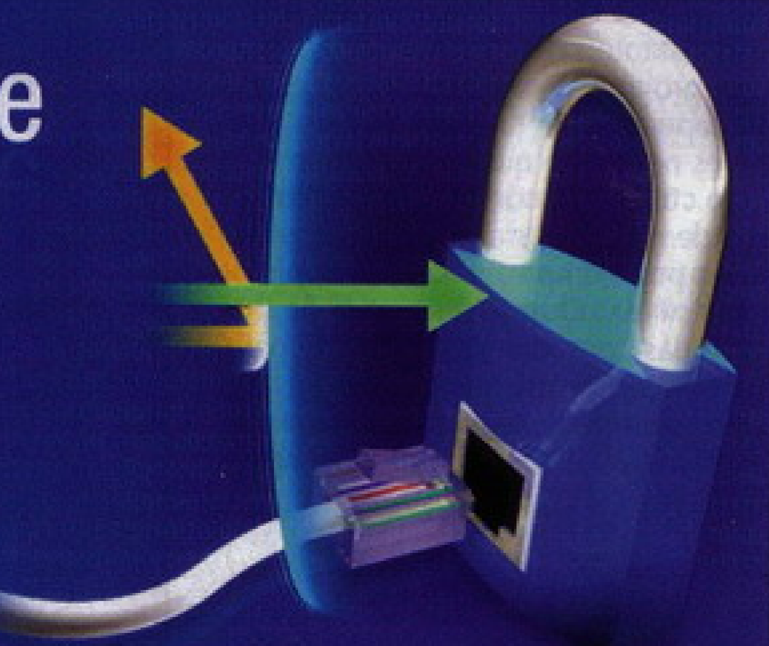


BREACH

Home Projects Documentation Download Training Contact About Breach Security



ModSecurity for Apache v2 is now available. The exciting new features include XML support, event correlation, transaction scoring, anomaly detection, data persistence, a wealth of anti-evasion functions, regex back-references, support for sessions, and many more. This release further increases the flexibility of the core engine and enables you to do *what* you want *exactly when* you want it.



News and Updates

ModSecurity 2.1.2
(August 6, 2007)
ModSecurity for 2.1.2 is a patch release that fixes several small issues discovered in previous versions and upgrades the bundled rules to the latest Core Rules version.

Projects

The following projects are hosted on this web site:

- ModSecurity for Apache
- ModSecurity Core Rules
- ModSecurity Console
- Cool Rules

Web Security Blog

www.modsecurity.org/blog

August 31
Web Services Security
NIST has released a new guide on securing Web Services. It is a pretty good read for anyone who is planning to run WS,

LA PRIMERA PREGUNTA QUE VIENE A LA CABEZA ES EL FUNCIONAMIENTO DE LA COMUNICACIÓN ENTRE EL ATACANTE Y LA VÍCTIMA PARA PODER CREAR EL CANAL DE COMUNICACIÓN, YA QUE, A PRIORI, UNA CONEXIÓN DIRECTA ES TOTALMENTE INVIABLE

la web maliciosa, quedando todas las demás fuera del alcance de la infección.

La primera pregunta que viene a la cabeza es el funcionamiento de la comunicación entre el atacante y la víctima para poder crear el canal de comunicación, ya que, a priori, una conexión directa es totalmente inviable. Pues bien, la solución adoptada en este caso es realizar una conexión reversa, es decir, es la víctima quien se comunica, sin saberlo, con un servidor del atacante. Entonces al atacante le bastará con enviar las órdenes a ese servidor suyo y los clientes infectados se encargarán de leerla y enviar los resultados. Digamos que se trata de una comunicación a tres bandas, el esquema se puede ver en la figura1. A continuación veamos un poco mejor como funciona todo esto.

XSS-Shell

XSS-Shell esta formado por dos componentes, el que infecta y el que se encuentra en el servidor del atacante. Todo el código esta escrito en ASP .NET y VBS, consecuentemente, el servidor donde se encontrará el motor de la comunicación (XSS Shell server) deberá ser sobre Windows con .NET Framework 2.0 (mínimo). XSS Shell permite, además, configurar una contraseña para acceder al panel de administración. De esta manera la aplicación no puede ser vista por nadie sin el consentimiento expreso del propietario, además de evitar el robo de víctimas entre atacantes.

El proceso de infección es el siguiente:

1.- Se configura el servidor de XSS-Shell.

2.- Se realiza la inyección en una web o bien se postea un Link malicioso en algún foro.



3.- Se espera a que algún usuario caiga en la trampa.

En el primer paso se deberá configurar una contraseña segura para evitar accesos de terceros. El segundo paso es el más importante, ya que para que tenga éxito el ataque debe haber una alta probabilidad de que algún usuario pulse sobre el link malévolo. Finalmente, para el paso tres, bastará una alta dosis de paciencia. Después de realizar estos tres pasos se tendrá el control del navegador, más en concreto, de la pestaña a través de la cual se estuviera navegando y que se hubiera empleado para entrar en la web maliciosa. Las funcionalidades que ofrece de momento la aplicación se muestran en la tabla 1. Éstas han sido extraídas del manual que se ofrece en la propia web.

De esta lista se puede deducir lo peligroso que puede llegar a ser infectarse con una inyección de este tipo. Si el atacante tiene las herramientas adecuadas, simplemente el poder obtener cualquier cookie de la víctima ya proporciona acceso a infinidad de posibilidades. Como acceder a áreas privadas de las aplicaciones a las que se conecte habitualmente el usuario atacado.

XSS-Tunnel

Esta herramienta, como ya se ha comentado anteriormente, se sirve de las funcionalidades ofrecidas por XSS-Shell para llevarlas un poco más allá y acabar utilizando la víctima como proxy. El proceso necesario para la utilización de esta herramienta es prácticamente el mismo que se ha comentado anteriormente para XSS-Shell.

Así pues, partiendo de que ya se ha realizado la infección y se ha configurado XSSShell, ahora bastará con arrancar el programa de control que se proporciona en el paquete, en concreto 'XSSTunnel/XSS Tunnel Binary Release/XSSTunnel.exe'.

Una vez arrancado aparece una ventana igual a la que se puede observar en la imagen4. Ésta ha sido sacada del propio manual que se puede descargar desde la web del proyecto.

Observando las opciones que aparecen en la captura se aprecia la configuración general del programa. Por un lado tenemos la configuración del servidor propiedad del atacante para la comunicación (www.xssshellserver.com:6000/admin) junto con el password utilizado para la autentificación, y por otro lado, se encuentra la configuración del Proxy que, en este caso, quedará a la escucha en el puerto 8080, y accesible desde cualquier interficie de red.

Después de configurarlo todo bastará esperar a que alguna víctima se conecte al site señuelo y configurar nuestro navegador para que utilice como proxy

XSS-TUNNEL SE SIRVE DE LAS FUNCIONALIDADES OFRECIDAS POR XSS-SHELL PARA LLEVARLAS UN POCO MÁS ALLÁ Y ACABAR UTILIZANDO LA VÍCTIMA COMO PROXY

Tabla1

Get Cookie	Devuelve la cookie de la víctima de un dominio al azar.
Get Current Page	Devuelve la página actual.
Execute custom Javascript	Ejecución de código javascript arbitrario.
Get Mouse Log	Devuelve los movimientos del ratón.
Get Keylogger Data	Devuelve las teclas presionadas en la pestaña infectada.
Get Cllipboard	Devuelve el contenido del portapapeles de la víctima.
Get Internet IP Address	Devuelve la IP de la red local de la víctima.
Check Visited links	Verifica si ha visitado ciertas páginas basándose en el hack del CSS *
Crash Browser	Cierra el navegador de la víctima.

* CSS Hack: Hace algunos meses se hizo famosa una técnica para saber las páginas que habían sido visitadas por un cliente. El hack consiste en realizar una lista de los enlaces que se quieran comprobar, asociarles código CSS con la finalidad de que se pinten de un color diferente los links visitados. Al nterpretar este código el navegador si los links se encuentran en el history los marca de otro color. Finalmente basta con comprobar el color de cada uno de los enlaces mostrados para deducir los que se han visitado. El problema de esta técnica es lógico, si el atacante no conoce el dominio por el que ha estado la víctima, nunca lo descubrirá.



el servidor creado por XSSTunnel. Una vez realizadas estas acciones ya será posible navegar utilizando el navegador de la víctima, pudiendo controlar siempre la operación desde el programa XSSTunnel.exe tal y como se muestra en la imagen5, que forma parte también del manual disponible en la web. En ella se pueden observar las URL's que se han ido cargando a través del proxy.

Gracias a esta aplicación es posible acceder a áreas restringidas o hacernos pasar por la víctima con todos sus privilegios. Si un administrador de una entidad importante cayera en una trampa de este tipo, no sólo estaría comprometiéndose a él, si no que además pondría en peligro la seguridad entera de la empresa, ya que el atacante podría modificar tantos aspectos como los privilegios de su perfil permitieran.

SOLUCIONES Y PRECAUCIONES

Para abordar este problema se deben plantear dos puntos de vista: el del servidor por una parte y el del cliente por otra. Como se deduce de esto, la responsabilidad del problema recae en el propietario del servidor o de las aplicaciones que contienen webs vulnerables a inyección de código. Hay que decir que este tipo de vulnerabilidad es la primera en el ranking 2007 de vulnerabilidades realizado por la organización OWASP (http://www.owasp.org - Open Web Application Security Project), así que es bastante numeroso. Así pues, para protegerse de este tipo de ataque existen fundamentalmente dos estrategias a elegir, aunque se deberían usar conjuntamente.

La primera consiste en realizar una programación web segura y evitar este tipo de vulnerabilidades. Esta tarea no es tan fácil como puede parecer ya que actualmente el Cross-Site Scripting tiene tantas variantes que hace muy difícil la posibilidad de prevenirlas todas. Por este motivo entra en juego la segunda estrategia, que consiste en instalar un firewall de aplicación que se encargue de analizar las peticiones entrantes y salientes en busca de código malicioso, detectando así muchos de los ataques.

Un firewall de aplicación no deja de ser un proxy que interviene el tráfico antes de llegar al CGI y/o antes de ser enviado y lo analiza en busca de código malicioso o fugas de información, por ejemplo.

Existen varios, pero se va a hablar de uno distribuido bajo licencia GPL y que puede integrarse con el servidor web Apache, que es el servidor más extendido en entornos *nix.

Se denomina 'mod_security' y puede descargarse desde el siguiente enlace (ver imagen6):

www.modsecurity.org

En esta web, además, se encuentran disponibles multitud de documentos explicando el funcionamiento y configuración. La configuración se basa en expresiones regulares que hacen saltar las alarmas en caso de que se cumplan, estas afectan a toda la petición http, desde el User-Agent hasta el contenido web, petición POST, GET... eso permite que sean muy personalizables y, por lo tanto, adaptables a cada situación del servidor en particular a un nivel granular tan afinado como se quiera.

- Desde aquí aconsejo un paseo por dicha web para comprender mejor como esta estructurado todo el proyecto.

Finalmente se encuentra el cliente, que es objetivo de ataques y engaños por su inocencia y otras veces, es víctima de un ataque por un fallo de programación cometido en un servidor, con lo que el usuario se infecta sin darse cuenta de nada en absoluto, en este caso hablaríamos de mala programación. Para el usuario también existen utilidades para protegerse, de hecho, actualmente los propios antivirus ya incorporan sistemas de detección de inyecciones a través de Internet, analizando el trafico entrante y saliente al mismo tiempo que se procesan los ficheros bajados desde la red en busca de código vírico. Desafortunadamente la totalidad de antivirus no integran estas funcionalidades, y algunos que dicen hacerlo, no acaban de implementarlo de forma muy fiable. Además, también se ofrecen plugins para navegadores como Firefox que previenen ante este tipo de ataques analizando las peticiones, aunque aun así no se debe estar del todo seguros.

Una ultima recomendación sería, en última instancia, desactivar el javascript, de esta forma se evita la infección, aunque por otra parte no se apreciarán los detalles 'dinámicos' hechos en este lenguaje.

CONCLUSIONES

Después de estas pinceladas sobre las posibles aplicaciones del XSS, seguro que a nadie se le escapa la importancia de una buena protección frente a estas amenazas.

Desde aquí os recomiendo que probéis en vuestras propias carnes una inyección de este tipo, teniendo en cuenta que gracias a 'portcullis-security' se encuentra disponible una buena "suite" de utilidades. Así que bastará con instalar un IIS en vuestra red local junto con XSSTunnel y probarlo en vivo. En la web de los autores se puede encontrar vídeos demostrativos del uso e instalación de XSS Shell y XSS Tunnel, no tienen desperdicio. De esta manera se podrá comprobar la seguridad del entorno más cercano y se comprobará cómo no se está tan seguro como uno pueda creer.

Si alguno creía que simplemente navegando no podía pasar nada, que se lo replantee, ya que cada día salen nuevos métodos y técnicas para ridiculizar tanto al usuario como a las empresas de antivirus y protecciones de Internet y ponerles en jaque.

¡Saludos y hasta otra!

Por: Ferran Pichel
<fpichel@isecauditors.com>

FINALMENTE SE ENCUENTRA EL CLIENTE, QUE ES VÍCTIMA DE UN ATAQUE POR UN FALLO DE PROGRAMACIÓN COMETIDO EN UN SERVIDOR, CON LO QUE EL USUARIO SE INFECTA SIN DARSE CUENTA DE NADA EN ABSOLUTO, EN ESTE CASO HABLARÍAMOS DE MALA PROGRAMACIÓN

CURSO de HACKING

Hackeando con Google IV:

Introduciéndonos en un servidor MySQL

Llevamos tiempo sin dedicarle mucho espacio a las noticias más interesantes de hacking que han ido apareciendo, así que este mes vamos a poneros al día. Además vamos a aprovechar las noticias para explicaros cómo lograr colarnos en un servidor MySQL mal protegido.

Aprovechando que este mes tenemos a Google entre las noticias (y que la última vez que lo estrujamos fue en la entrega 99), vamos a ver cómo aprovechar la potencia de su buscador para localizar, ya de paso, websites con ficheros privados accesibles. Dado que andamos mirando temas de SQL podemos buscar ficheros que nos den el login y password de su base de datos. Para hacer esto buscaremos la siguiente cadena:

```
filetype:inc intext:mysql_
connect
```

Eso buscará ficheros .INC (que viene de include –incluir–) donde los programadores ponen funciones muy utilizadas en su web, entre las que se encuentran, claro está, las consultas a su base de datos.

Concretamente nos interesan los ficheros que contengan "mysql_connect", que denota que a continuación vendrán los datos de acceso :-)

Dentro del contenido del fichero *.inc os podéis encontrar, por ejemplo, esto:

```
$mysq_user = "root";
$mysql_user_pw = "clave";
$mysql_host = "localhost";
$mysql_db = "dev";
$link = mysql_
connect($mysql_host, $mysq_
user, $mysql_user_pw);
```

O algo tipo esto:

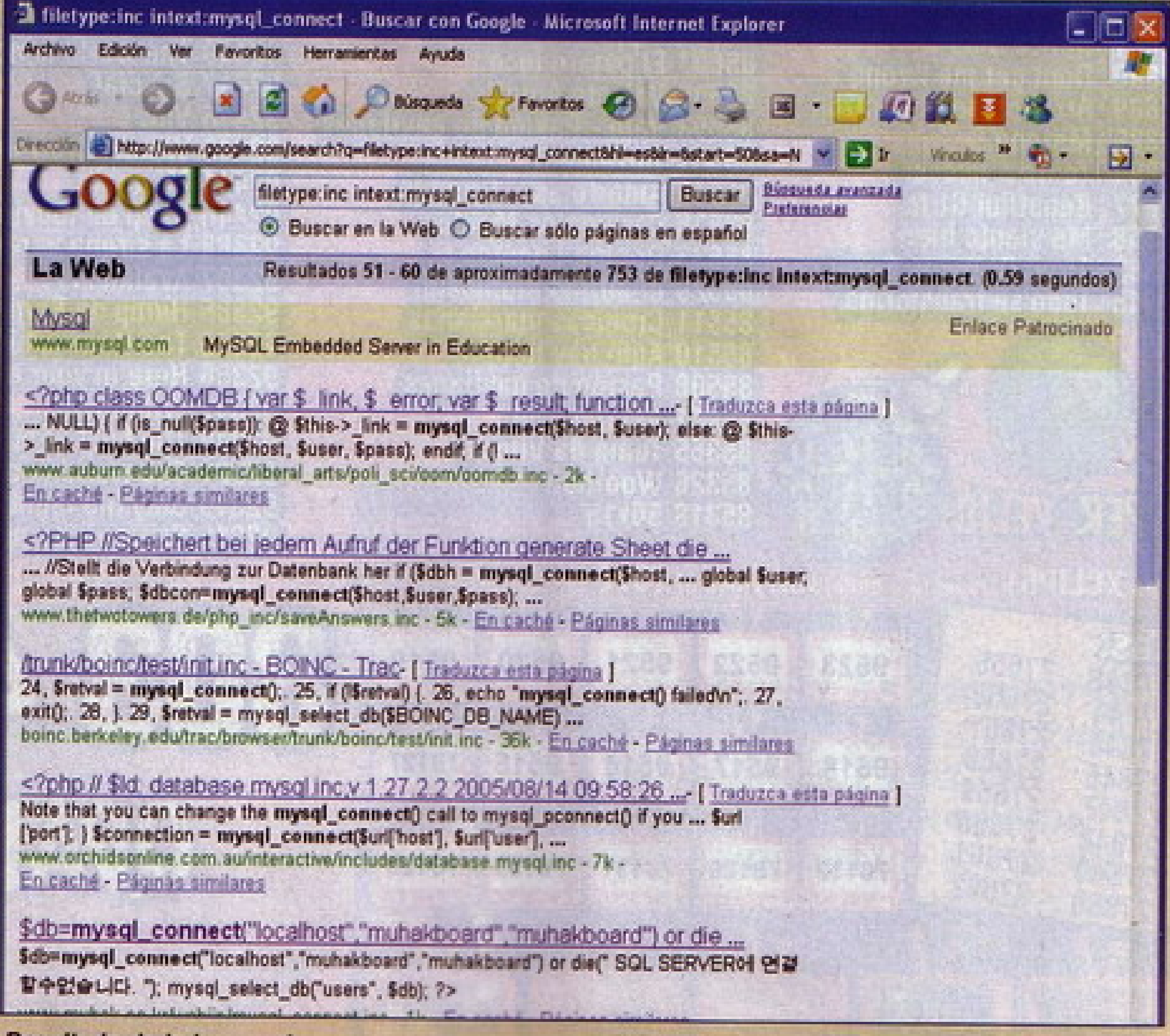
```
$CON = mysql_
connect('localhost', 'root',
'clave');
$DB = mysql_select_
db("dev", $CON)
```

De hecho, es posible que el mismo Google os haya hecho el favor de mostraros el contenido del fichero que os interesa. Es decir, ¡podéis conocer el nombre de usuario y contraseña del servidor sin necesidad de tocarlo si quiera! En el ejemplo eso lo veis para el último resultado que aparece.

En caso de no ser así, tendréis que ir pulsando en los enlaces para ir buscando la información que os interesa. Si os encontráis con algo tipo:

```
<?php
include('functions.php');
$link = mysql_
connect($dbserver, $dbuser,
$dbpass);
   mysql_select_db($dbdata);
```

Eso significa que la aplicación coge los valores de la base de datos de unas variables que ha cargado previamente (las variables son las que aparecen precedidas por el símbolo del dólar). Esas variables las habrá cargado seguramente del dichero "functions.php" a cuyo contenido vosotros no tendréis acceso, porque el servidor web



Resultado de la busqueda.



no os mostrará el contenido de un fichero PHP, sino que lo interpretará (y no creo que el desarrollador haya sido tan tonto como para que esos datos tan críticos se muestren en vuestro navegador, tendría que hacer que se mostraran a propósito).

Resumiendo, que ese tipo de ficheros no os interesa, pero no desfallezcáis ya que aunque en la previsual de Google os aparezcan variables y no la password hard coded (es decir, introducida en el propio código), es posible que cargue los datos de un "functions.inc", en cuyo caso cargaríamos dicho fichero y a volar :-) o que las variables donde se almacenan los datos estén en el mismo fichero, pero en líneas distintas y por eso Google no las muestra en la previsual. ¡Hay que intentarlo todo!

Imaginemos que hemos encontrado el fichero en http://www.server.com/mysql.inc.

Está claro que lo que nos interesa de ahí es el nombre de usuario y contraseña. Aunque lo muestren de distintos modos el orden siempre es el mismo:

1º Dirección del servidor MySQL: En el ejemplo es "localhost", es decir, que la web se conecta a su propia máquina (luego la IP del servidor MySQL es la misma que la de la web), en el caso de la captura de pantalla la máquina a la que nos tendríamos que conectar es www.muhak.co.kr (no lo intentéis porque tiene el puerto bloqueado, si no no lo pondríamos aquí como ejemplo jejeje), y en nuestro ejemplo sería www.server.com.

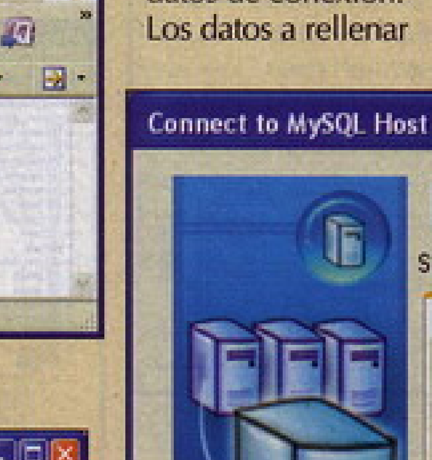
2º Nombre de usuario: En el ejemplo es "root".

3º Contraseña: En el ejemplo es "clave".

4º Base de datos: En el ejemplo es "dev".

Lo siguiente que tendríais que hacer, una vez obtenidos los datos de acceso, sería utilizar un escaneador de puertos para ver si el puerto TCP 3306 del MySQL está abierto.

Si es así, ahora toca conectaros. Para ello utilizaremos un programa específico, el SQLyog Community Edition, que es gratuito. Os lo dejamos en SQLyog611.exe. Su instalación no tiene ningún secreto. Una vez lo hayáis terminado de instalar, ejecutadlo y no le hagáis caso a la pantalla que os ofrece comprar la versión Enterprise (pulsad en "Continue")... a no ser que os encante el programa y queráis darle un uso más profesional.



La primera pantalla os pedirá los datos de conexión. Los datos a rellenar son los que habéis obtenido del fichero .INC, además de la BD en cuestión a la que os tendréis que conectar.

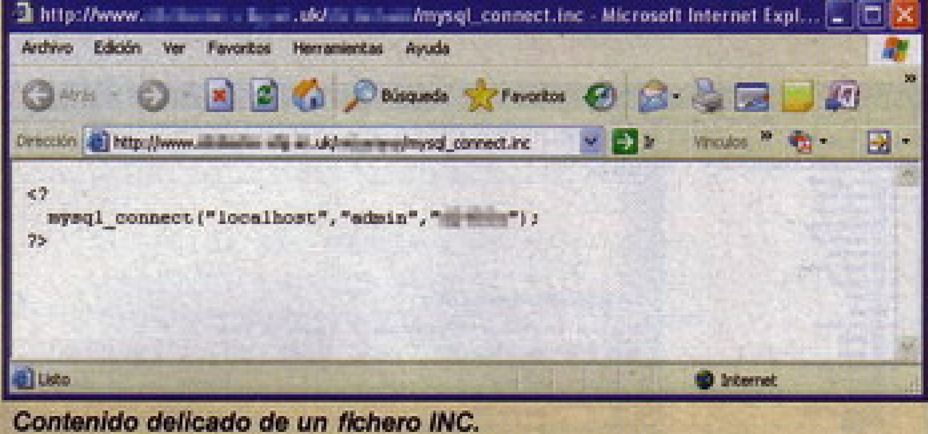
Listo, pulsamos ahora en "Connect". No penséis que con tener los datos de acceso y el puerto abierto está todo hecho, ahora queda comprobar si permite que el usuario que hemos cazado tiene permiso para acceder desde nuestro ordenador (MySQL en este sentido permite bastante nivel de detalle con respecto a los permisos). Si el usuario que estamos utilizando no permite que se conecte desde cualquier lugar, obtendremos uno de estos mensajes de error:

1.- Host '[tu IP]' is not allowed to connect to this MySQL server: Significa que los datos de acceso son correctos, pero que no nos permite acceder desde nuestra IP (tal vez sólo permita conexiones desde la propia máquina, que es donde está la web que hace uso de esa BD).

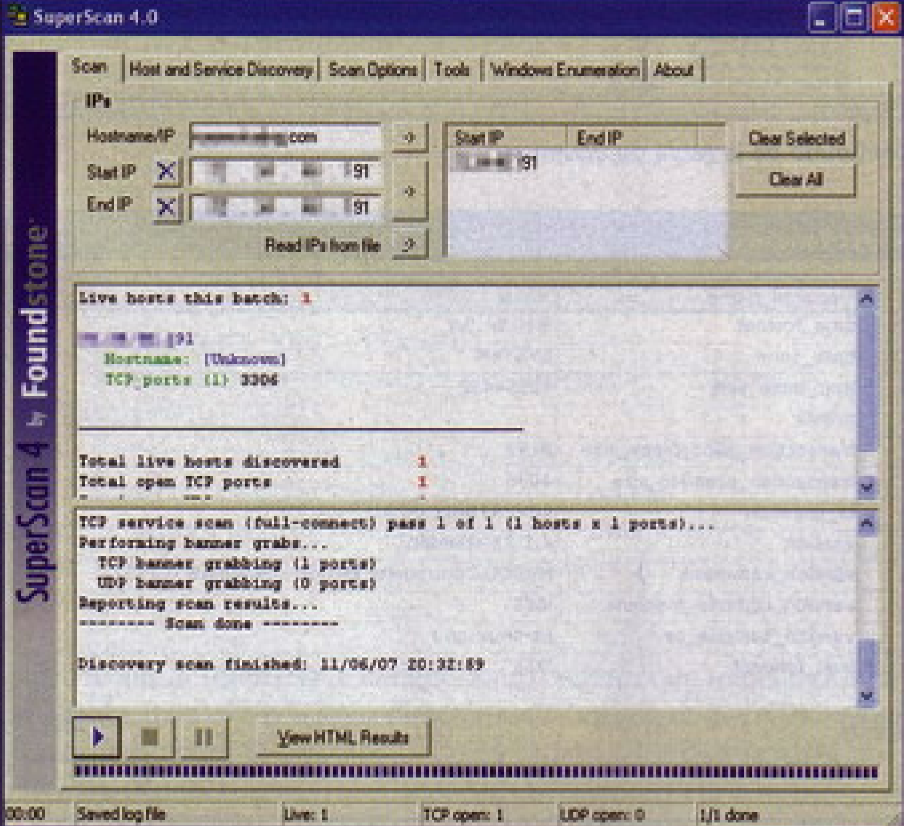
2.- Access denied for user 'root'@'[tu IP]' (using password: YES): Significa que el usuario o la contraseña son incorrectos (tal vez el servidor MySQL se encuentra en otra máquina).

Si el mensaje de error os aparece en castellano, por ejemplo, ya sabréis en qué idioma está configurado el servidor MySQL.

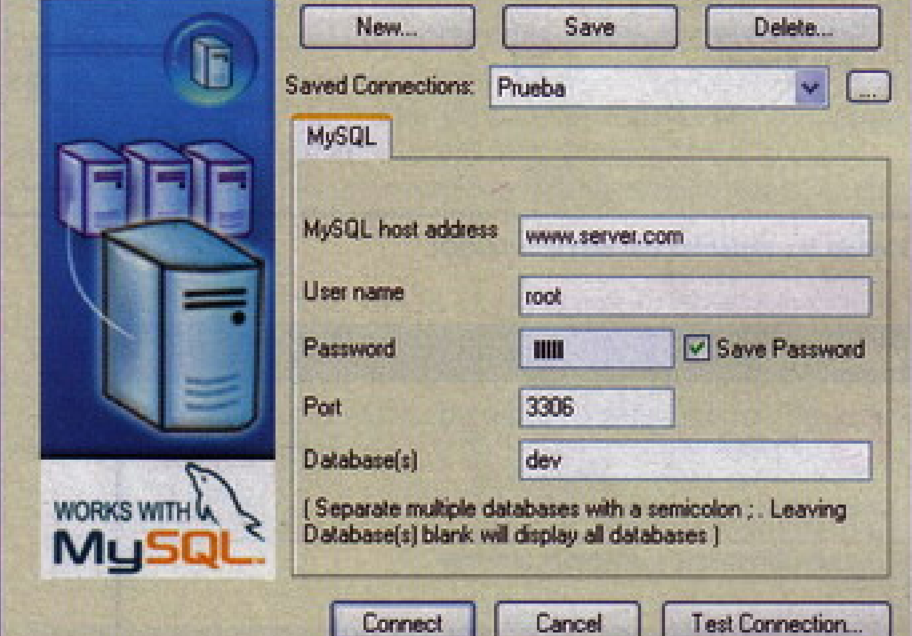
Pero si todo ha ido bien, nos aparecerá la BD a la que nos hemos conectado fe-



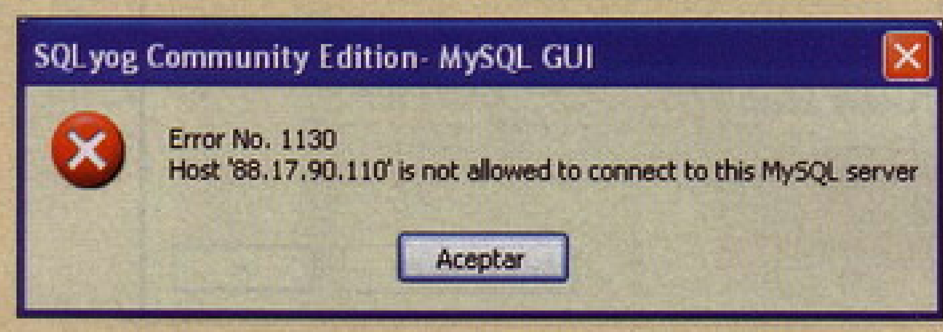
Contenido delicado de un fichero INC.



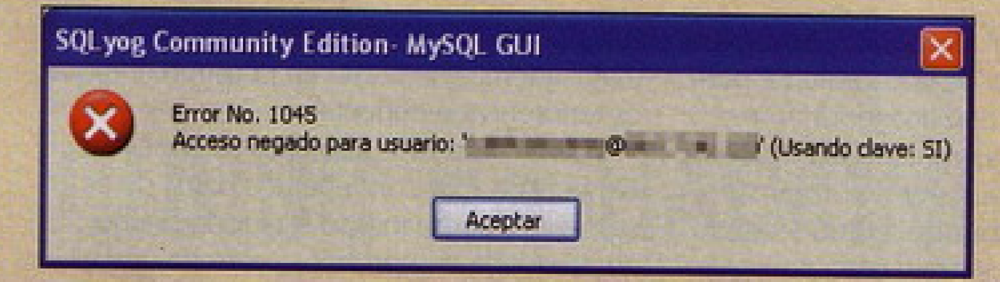
Detección de un equipo con el puerto 3306 abierto.

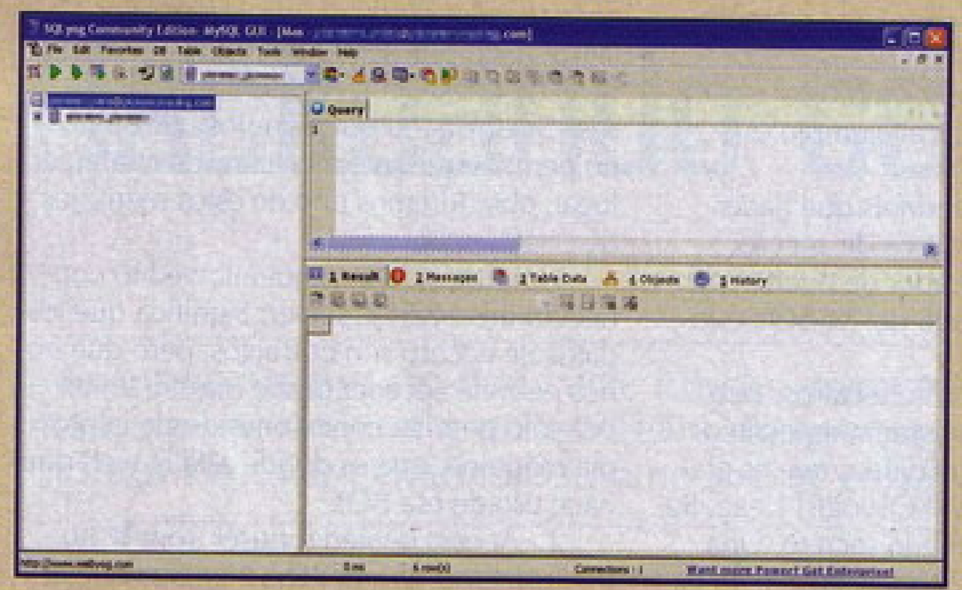


Configuración de la conexión al MySQL.

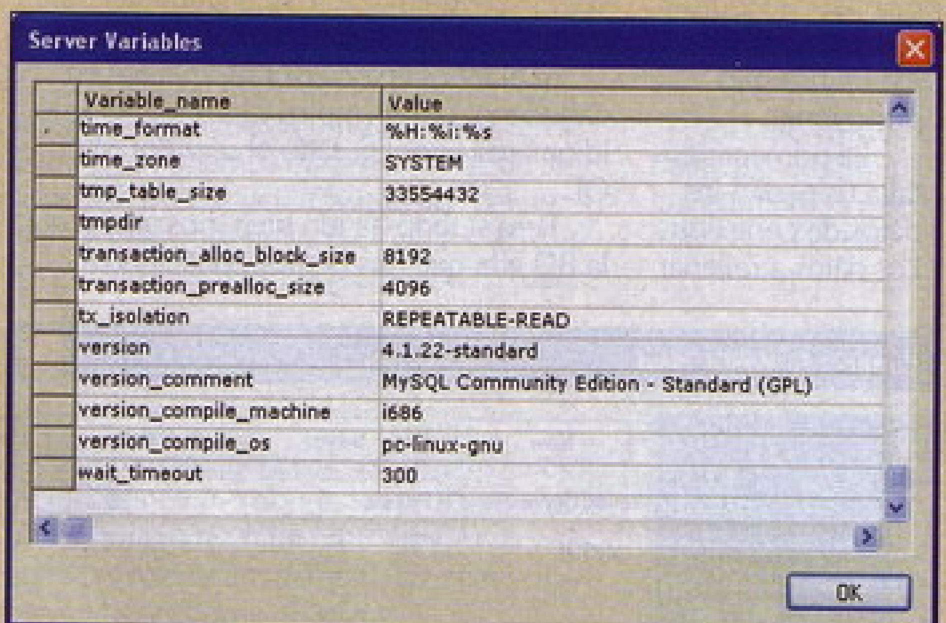


Mensaje de prohibición de conexión al MySQL.



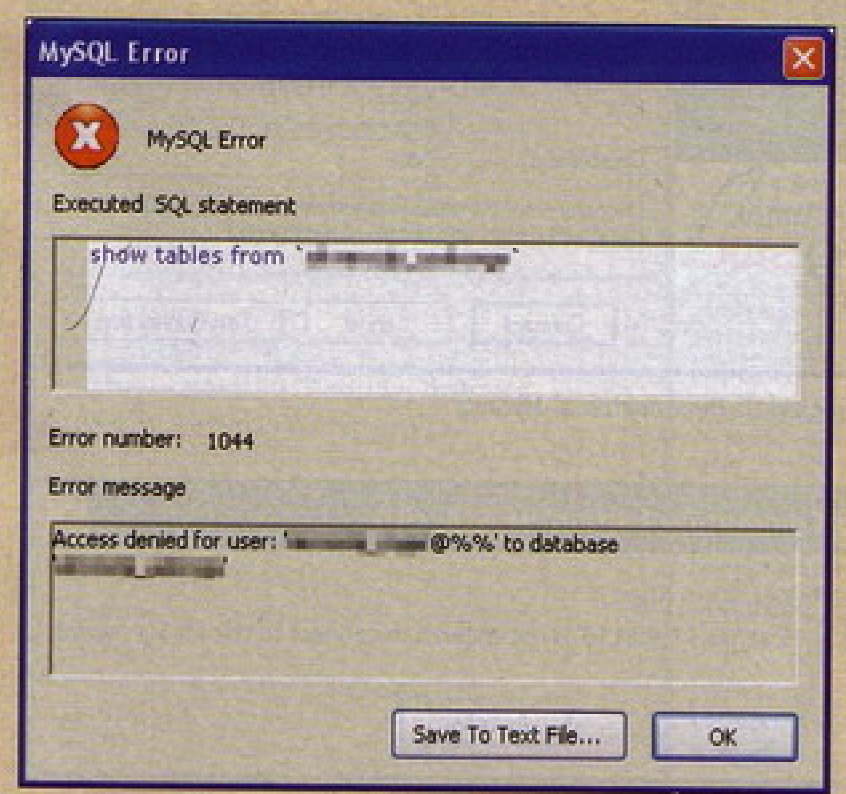


Conexión al MySQL.



Variable_name	Value
time_format	%H:%i:%s
time_zone	SYSTEM
tmp_table_size	33554432
tmpdir	
transaction_alloc_block_size	8192
transaction_prealloc_size	4096
tx_isolation	REPEATABLE-READ
version	4.1.22-standard
version_comment	MySQL Community Edition - Standard (GPL)
version_compile_machine	i686
version_compile_os	pc-linux-gnu
wait_timeout	300

Viendo las variables del servidor MySQL



Mensaje de error.

lizmente a la izquierda. Veréis el nombre_de_usuario@servidor y, colgando de él, la base de datos.

Si queréis conocer detalles sobre el servidor SQL pulsad en Tools - Show - Variables. Ahí podréis conocer los detalles de la configuración del servidor SQL, entre los que encontraréis información sobre rutas de directorios (que os permitirán conocer si está instalado en un Linux o en un Windows rápidamente), versión del motor, etc.

Para ver las tablas que contiene, tenéis que desplegar la BD. Llegados a este punto nos podemos llevar un nuevo chasco: Access denied for user: 'root@%' to database 'dev'

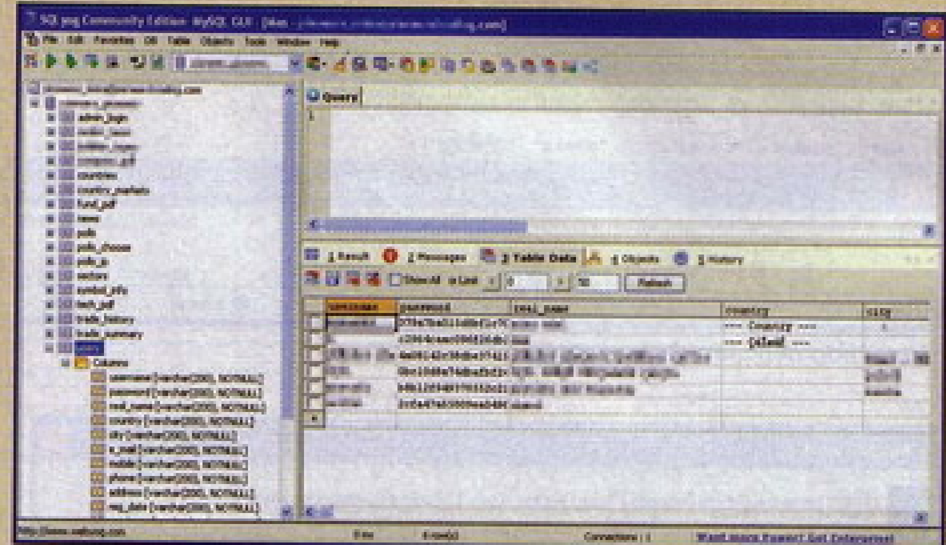
Esto ocurre si nos hemos equivocado de base de datos y ésta no existe.

Pero si tenéis suerte y podéis desplegar la BD podréis ver las tablas que contiene ¡ya era hora de que lo vierais, después de tanta inyección de SQL!

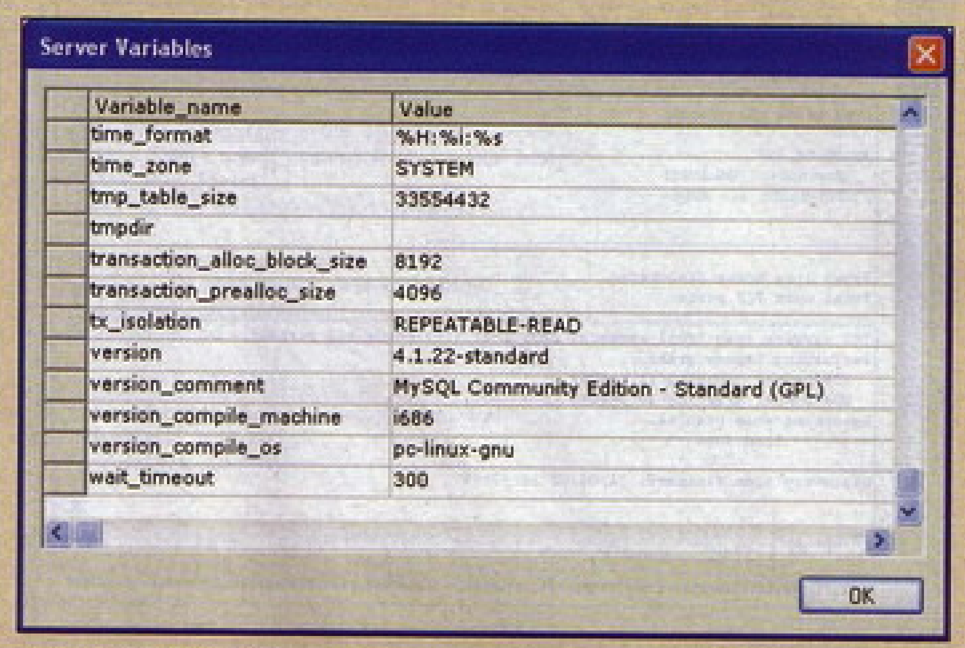
Luego, si desplegáis cada tabla veréis la carpetita "Columns", que muestra las columnas y el tipo de datos que se almacena en ellas. Si queréis ver lo que se almacena en una tabla, seleccionadla y, a continuación, pulsad en la ventana de abajo a la derecha sobre la pestaña "Table Data". El programa se ocupará de listar todo el contenido de dicha tabla (más bien las 50 primeras filas, que es lo que está definido por defecto).

Si cliqueáis sobre cualquier celda, podréis cambiar el valor de los datos almacenados en la BD. Pero ya sabéis una cosa ¡nunca se os ocurra estropear nada! De todos modos los cambios no se producen hasta que se pulsa en el icono del disquete (Save changes), mientras tanto os avisa de que no se han guardado los cambios con el mensaje "Data modified but not saved".

Algo que encontraréis muy instructivo es al pulsar en la pestaña "History", ya que os muestra las sentencias SQL que ha ejecu-

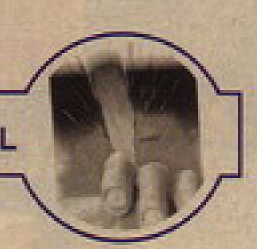


Contenido de la tabla de usuarios.



Variable_name	Value
time_format	%H:%i:%s
time_zone	SYSTEM
tmp_table_size	33554432
tmpdir	
transaction_alloc_block_size	8192
transaction_prealloc_size	4096
tx_isolation	REPEATABLE-READ
version	4.1.22-standard
version_comment	MySQL Community Edition - Standard (GPL)
version_compile_machine	i686
version_compile_os	pc-linux-gnu
wait_timeout	300

Exportando una BD.



Asignando permisos para tablas.

tado la aplicación para hacer lo que queríais (listar el contenido de una tabla, modificar un valor, etc.).

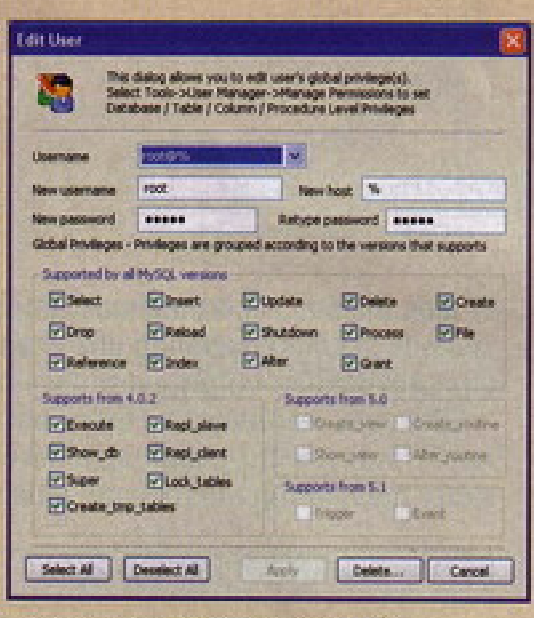
Si queréis realizar una copia de la base de datos pulsad en Tools - Backup database as SQL dump. Si dejáis las opciones por defecto, será como si realizarais un backup de la misma, es decir, que luego podríais restaurarla en cualquier sitio, incluso en vuestro propio PC :-)

El contenido del fichero de backup será algo similar a lo siguiente:

```
/*
SQLyog Community Edition- MySQL GUI v6.11
MySQL - 4.1.22-standard : Database - dev
*****************************************
*/
/*!40101 SET NAMES utf8 */;
/*!40101 SET SQL_MODE=''*/;
create database if not exists `dev`;
USE `dev`;
/*!40014 SET @OLD_FOREIGN_KEY_CHECKS=@@
FOREIGN_KEY_CHECKS, FOREIGN_KEY_CHECKS=0 */;
/*!40101 SET @OLD_SQL_MODE=@@SQL_MODE, SQL_
MODE='NO_AUTO_VALUE_ON_ZERO' */;
/*Table structure for table `admin_login` */
DROP TABLE IF EXISTS `admin_login`;
CREATE TABLE `admin_login` (
  `admin_id` bigint(20) NOT NULL auto_
increment,
  `admin_user` varchar(255) default NULL,
  `admin_pass` varchar(255) default NULL,
  `admin_type` varchar(255) default NULL,
  PRIMARY KEY  (`admin_id`)
) ENGINE=MyISAM AUTO_INCREMENT=10 DEFAULT
CHARSET=latin1;
/*Data for the table `admin_login` */
insert  into `admin_login`(`admin_
id`,`admin_user`,`admin_pass`,`admin_type`)
values (1,'admin','21232894a0e4a80f297a57a5a743
1fc3','all');
```

Si tenéis la suerte de acceder con un usuario que tenga todos los privilegios para el MySQL, o directamente conseguís acceder con el usuario root, podréis también darle un repaso a los usuarios del SGBD. Para ello id a Tools - User Manager ⊠ Manage Permissions.

Ahí os mostrará, en la primera zona, los usuarios existentes en el SGBD. Una vez que seleccionéis uno, os aparecerán las tablas a las que tiene acceso en la segunda zona. Si seleccionáis una de las tablas, os mostrará las columnas de la misma en la tercera zona. Para cualquiera de estos podéis seleccionar los permisos que queráis que tenga. Os lo vuelvo a recordar ¡¡¡no se os ocurra estropear nada!!! Para practicar tenéis vuestro ordenador, ahí podéis montar lo que queráis (a ver si vais a entrar como un elefante en una cacharrería y la liamos).



Asignando permisos generales.

Nuevamente, hasta que no pulséis el botón "Apply", no se aplicarán los cambios que hayáis hecho.

Si lo que queréis es controlar los permisos en general del usuario, deberéis ir a Tools ⊠ User Manager ⊠ Edit User. Desde aquí podréis asignar permisos como el de que el usuario pueda asignar permisos a otros usuarios (grant).

Si os preguntáis por qué el usuario aparece como "root@%" os lo explico. Tras el nombre de usuario, y separado mediante una arroba, se puede especificar la IP de origen del usuario que estará autorizada a conectarse. MySQL interpreta el símbolo "%"como si fuera "*", lo que viene a significar que el usuario root puede acceder desde cualquier lugar.

Incluso podéis especificar permisos en función del origen de la conexión, así podéis seleccionar el usuario "root@localhost" (lo que se traduce en que el usuario root se conecta desde el propio servidor) para definir sus permisos cuando se conecta desde la máquina que hace de servidor.

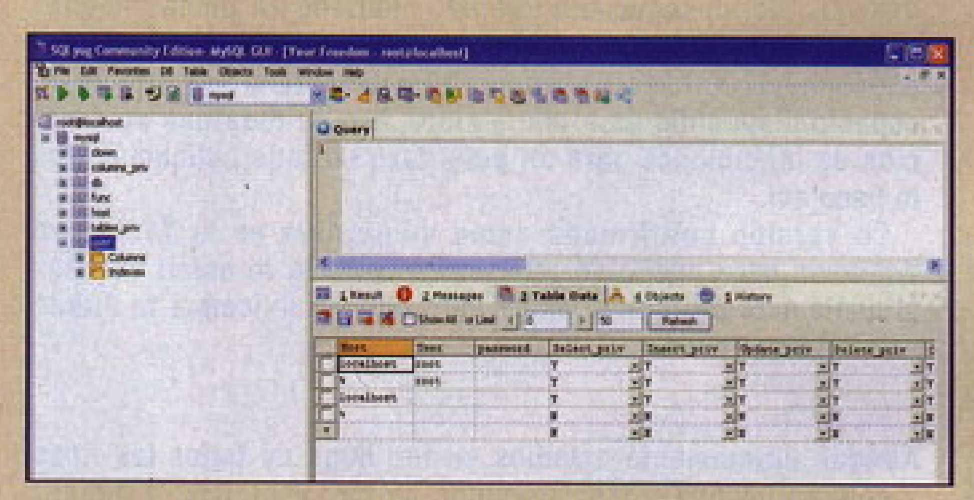
Si lográis tener todos los permisos, podréis conectaros a la BD "mysql", que es la que lo controla todo. Para ello cread una nueva conexión, especificad el usuario que tiene todos los permisos y luego indicad como base de datos "mysql".

Por sorprendente que os pueda parecer, todavía hay servidores MySQL que tienen, para el usuario root, la clave "root" o vacía. Si queréis probar a descubrir estos servidores probad a buscar en Google:

```
Warning: mysql_connect(): Access denied for
user 'root' (Using password: NO)
```

Una vez localizadas webs con este mensaje de error, bastará con probar a conectarnos...

Andrés Méndez Barco
Manuel Baleriola Moguel



Accediendo como root a mysql a través de una conexión anónima.

Bugy Bugy

El mes pasado recordábamos un poco el vocabulario específico de la sección haciendo una especie de monográfico de bugs que provocaban buffer overflow y denegación de servicio.

Este mes veremos de todo, para Windows, para Linux, de Apple pero, como siempre, tendréis que seguir leyendo para saber más porque hasta aquí podemos leer.



Siempre la copia de seguridad

Está claro que es importante tener copias de seguridad de la información sensible que se tenga en un ordenador porque, el día menos pensado, siempre puede suceder una desgracia, sin daños personales por supuesto pero sí cuantiosos en cuanto a que muchas veces cierta información tiene un valor incalculable. Imaginad que perdéis las fotos de un viaje, de un evento único o el documento de un trabajo que estáis haciendo. Los backups son y serán siempre algo a tener en mente para no tener que lamentar nada en caso de catástrofe.

Hasta aquí todos de acuerdo, me supongo :P. Pero, ¿qué pasa cuando el programa de los backups tiene algún problema? Pues fácil, que aparece en esta sección como todos aquellos programas que tienen problemas.

En este caso el programa de backup afectado es el ARCserve Backup para portátiles y ordenadores de sobremesa. El problema, para no perder las buenas costumbres, un buffer overflow que permite a un atacante ejecutar código arbitrario con privilegios del sistema.

Para aquellos que manejen este programa, algunos detalles más del problema. El componente LGServer tiene varias funciones vulnerables que manejan peticiones de red, teniendo además cada una más de un fallito. El conjunto total de fallos asciende a más de 50 buffer overflows así que os podéis hacer una idea del desaguisado que hay montado en dichas funciones. La mayoría de las vulnerabilidades se deben a que se copia cosas al buffer sin chequear previamente si hay suficiente espacio disponible para ello y claro, eso es toda una declaración de intenciones para un petardazo en toda aplicación que lo hace así.

La versión confirmada como vulnerable es la 11.1 para Windows pero puede ser que otras también lo estén así que, si usáis este programa, mejor será que actualicéis a la última versión disponible.

Una de pingüinos

Aunque últimamente estamos viendo bugs de todos los tipos y colores, siempre habrá algunos que os dediquéis a debatir



sobre qué sistema operativo es más seguro o menos, que si Windows o Linux. Como muchas veces sacamos cosas de Windows, ahora le toca el turno a uno de Linux para que podáis seguir debatiendo sin descanso.

En esta ocasión la distribución afortunada es la Fedora Core 7, para los despistados, la que se puede decir que es la RedHat gratuita. El problema está en el driver ALSA que se incluye en el kernel de la distribución que permite a un atacante obtener información sensible de la memoria del kernel. La versión que seguro está afectada por este bug es el kernel 2.6.22.1 sin descartar que otras lo estén también.

Érase una vez una manzana

Si antes decíamos que veíamos un bug de Linux para que sigáis debatiendo entre qué sistema es mejor. Los terceros en discordia en ese gran debate son los usuarios de Mac de Apple. Precisamente de Apple vamos a hablar ahora ya que también tiene más productos aparte de los ordenadores y algunos tan famosos como el iPhone o iTunes o iPod, todo con una i seguida del nombre XD.

¿Y qué producto es el agraciado con el nombramiento bugy bugy de este mes de todos los que tiene Apple? ¿Será el famoso iPhone del que tanto se habla ahora? Pues no, nos tememos que este mes al menos no. En fin, no os vamos a tener en ascuas más y os lo vamos a decir. El producto seleccionado es iTunes, el reproductor multimedia de Apple que funciona en varias plataformas y mucha gente lo usa por la información que da sobre las canciones así como las funcionalidades que aporta. El fallo, pues que en la versión 7.3 tiene un desbordamiento de pila en la funcionalidad de las carátulas de álbum. Si lo usáis, actualizad que la versión 7.4 ya lo arregla.



LO MEJOR PARA TU MOVIL

MENSAJES AL 7477

Envia ARIMAG + EL CODIGO
al 7477 Ej: ARIMAG 50406







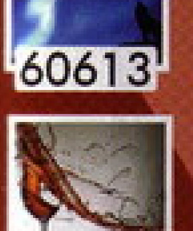




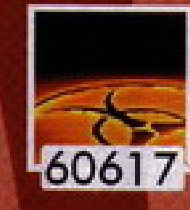




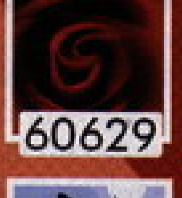


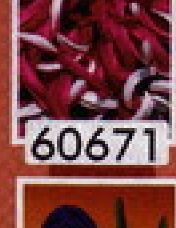




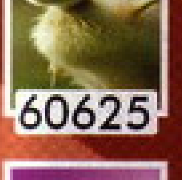



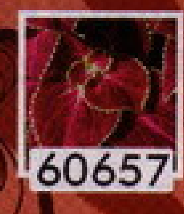






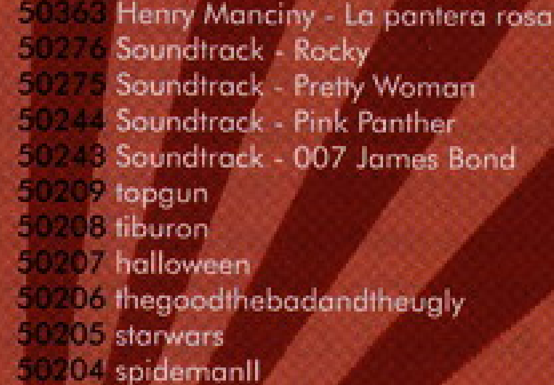

60162	60166	60163	60676	60169
60156	60135	60614	60673	60150
60326	60626	60604	60571	31585
60337	60336	60133	60351	40077
60613	1009	60349	60599	60660
60600	60350	60601	60609	60598
60612	60603	60620	60602	60617
60314	60629	60622	60619	60671
60625	60168	60161	60154	60171
60217	60210	60303	60289	60152
60649	60651	60656	60657	60674

Envia ARPOLI + EL CODIGO
al 7477 Ej: ARPOLI 50406

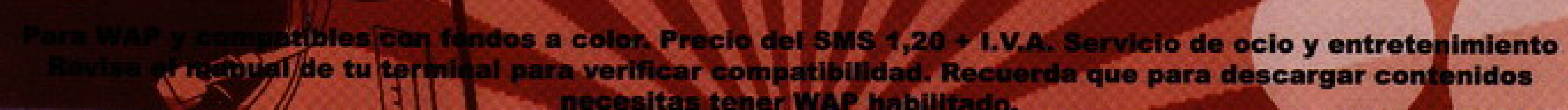


50406 Gorillaz - Dirty Harry
50393 Red Hot Chilli Peppers - Dani Ca
50375 Fito y Fitipaldis - Soldadito Marin
50374 Extremoduro - Golfa
50291 Freestylers feat. Petra - Told You
50264 Green Day - Wake Me Up When
50245 Moby - Dream About Me
50080 Simple Plan - Welcome My Life
50068 Green Day - Boulevard Of Broke
50063 Gorillaz - Feel good inc
50061 Weezer - Beverly Hills
50058 Good Charlotte - Just Wan Live
50312 The Chemical Brothers - Galva
50155 Fatboy Slim - Slash Dot Dash
50146 Neng - Soy persona
50145 Neng - Que pasa Neng
50134 Carlinhos Brown y Dj Dero
50046 Chemical Brothers - Believe
50388 El Koala - Opa yo viace un corra
50353 Mattafix - Big City Life
50352 La Cabra Mecanica - La uña de
50348 The Rolling Stones - Rain fall do
50346 Simple - Crazy
50343 Nickelback - Far Away
50342 Hoy no me puedo levantar - Un..
50341 Goldfrapp - Number one
50332 Pastora - Dia tonto
50330 Modestia Aparte - Cosas de la.
50329 Jamie Cullum - Mind trick
50321 Pain - Shut Your mouth V2
50318 El Barrio - Querida enemiga
50408 Jean Michel Jarre - Oxygene
50407 Hari Mata Hari - Lejla (Eurovis
50405 Fabrizio Faniello - I do (Eurovis
50404 Elena Risteska - Ninanaina (Eu
50403 Dima Bilan - Never Let You go
50400 Andre - Without Your Love (Eur
50391 Gypsy Kings - Hotel California
50390 Gloria Gaynor - I will survive
50389 Carlos Jeans - Have a nice da
50381 King Africa - Paquito el chocol
50380 Complices - LLámame
50379 Victor - The fool on the hill
50378 Zucchero y Mana - Baila more
50377 Scorpions - Winds of change
50376 Juanes - Nada valgo sin tu am
50372 Ennio Morricone - La muerte..
50370 Anastacia - Left outside alone
50369 Alberto Iglesias
50368 Sergio Rivera - Me Envenena
50366 Niña Pastori - Tu me camelas
50363 Edurne - Despierta
50360 Coti y Paulina Rubio - Otra vez
50359 Belanova - Me pregunto
50358 Tara Blaise - The Three degree
50355 Richard Ashcroft - Break the ni
50354 OT 2005 - Batlika Medley
50351 Kelly Clarkson - Behind these H
50350 Chambao - Sueño y muero
50349 Bono Feat. Mary J Blige - One
50345 Sidonie - Joe
50344 Pablo Moro - Vodka y caramel

Envia ARREAL + EL CODIGO
al 7477 Ej: ARREAL 50406



50397 Nina Simone - (Spot Audi A4)
50395 Marvin Gaye - (Spot Movistar)
50347 Andy Williams - (Spot Honda)
50338 Dennis MCCarthy - BSO V
50227 tangagirls
50223 nike_brasil
50222 martini
50212 cocacola
50383 Amelie BSO - La Valse Damelie
50382 Amelie BSO - Jy suis jamais alle
50363 Henry Manciny - La pantera rosa
50276 Soundtrack - Rocky
50275 Soundtrack - Pretty Woman
50244 Soundtrack - Pink Panther
50243 Soundtrack - 007 James Bond
50209 topgun
50208 tiburon
50207 halloween
50206 thegoodthebadandtheugly
50205 starwars
50204 spidemanII
50203 silenciodeloscorderos
50202 shrek2
50398 Pignoise - Nada que Perder
50368 Soundtrack - Revelde Way
50367 Soundtrack - Perdidos
50366 Soundtrack - Mujeres desespe.
50365 Soundtrack - Dr. House
50237 uefachampionsleagueofficia
50236 xfiles
50235 thesimpsons
50234 sesamestreet
50233 aquinohayquienviva
50232 knightrider
50231 willandgrace
50230 twinpeaks
50229 cheers
50228 teletubbies
50226 southparkth
50225 sensacion_vivir
50224 pokemon
50221 macgyver
50220 garfield
50219 flinstones
50218 familia_addams
50217 falconcrest

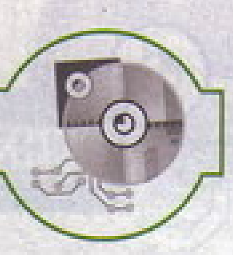


Para WAP y compatibles con fondos a color. Precio del SMS 1,20 + I.V.A. Servicio de ocio y entretenimiento Revisa el manual de tu terminal para verificar compatibilidad. Recuerda que para descargar contenidos necesitas tener WAP habilitado.



BACKTRACK

Salió de sus ensoñaciones abruptamente despertado por la vibración del aviso automático. Con un gesto de fastidio centró la proyección móvil sobre una zona de la pared que estuviera al alcance de su vista de una forma mas cómoda. Mientras respondía al mensaje recibido repasaba mentalmente en las posibles formas de reclamar y conseguir que la pantalla virtual le siguiera a él y no se escondiera en los rincones mas insospechados de la estancia. Hoy como a principios del siglo XXI, conseguir que un profesional realizara un trabajo de calidad era tan difícil como encontrar un diamante en el suelo a la salida de una reunión de políticos. Corrían los últimos días de 2067 y algunos problemas eran tan difíciles de resolver como hacia sesenta años.



El mensaje recibido no tenia gran importancia, pero tuvo la virtud de recordarle una tarea que desde hacia unos días le estaba esperando, pero que posponía una y otra vez. Algunos encuentran placer en revolver en las pertenencias de personas que han desaparecido pero a otros les resulta incómodo y a veces doloroso. En esta situación se encontraba Viajero Junior III. Cuando su abuelo desapareció a la razonable edad de 111 años no se interesó por lo que pudiera tocarle de la enorme herencia, solo se preocupó, desafiando las protestas de su mujer, que el resto de la familia no tirara nada antes que el pudiera revisarlo y decidir su destino. El resultado fue una continua afluencia de objetos, documentos, libros, publicaciones y paquetes que regularmente alguien de su extensa familia anunciaba su descubrimiento o directamente dejaba en su casa. Su abuelo había sido una extraña persona y lo que dejó tras de si daba fe de ello.

Hacía unos meses un sobrino le envió mensaje cifrada y certificado informándole que haciendo limpieza en un desván que pertenecía a una casa donde su abuelo gustaba de pasar las vacaciones, había encontrado toda una serie de ordenadores antiguos, libros y caja de material plástico que no había querido abrir. Junior III utilizó uno de sus días comodín que la regulación de trabajo le permitía utilizar a su antojo para tomar el transporte rápido de vecindad y hacer en hora y media los trescientos kilómetros que le separaban de su sobrino, para comprobar que los viejos ordenadores carecían de valor incluso para los coleccionistas, pero que los libros de autentico papel y la caja tenían su interés. El problema se le presentó para trasportar los objetos. En un mundo envejecido, tenia mas valor una hora de esfuerzo físico que cien de trabajo intelectual y los robots todavía seguían siendo una esperanza como hacia cien años. Finalmente consiguió un buen acuerdo con un inmigrante finlandés, fugitivo de los glaciares que amenazaban su pais, y mediante un precio razonable se avino a llevar los bultos hasta la conexión cercana de la unidad local de transporte publico y desde ahí le fue mas fácil conectar con el transporte de vecindad aunque, eso si, tuvo que soportar las desaprobadores miradas de todos los octogenarios que poblaban el vehículo que no entendían como alguien utilizaba un espacio dedicado al transporte de personas para mover simples bultos inanimados.

UN PRIMER VISTAZO

Encontró rápidamente sitio para los libros de autentico papel, cada vez mas raro, pero el contenido de la caja le dejó bastante perplejo, aunque ya estaba habituado a los extraños objetos que su abuelo se dedicó a atesorar sobretodo desde que su jubilación le dejó tiempo libre para dedicarse a unas actividades que su abuela consideraba como una total pérdida de tiempo, a pesar de que nunca hizo ascos a un dinero que entraba en la cuenta bancaria a una velocidad no justificada por el importe de su jubilación. El caso es que dentro de la caja y en un orden bastante inexplicable había una enorme cantidad de discos de plástico que rápidamente identificó como antiguos soportes para almacenar información.

El reconocer el soporte no le iba a ser de mucha ayuda para saber su contenido. Durante el primer tercio del siglo XXI se habían utilizado ampliamente diversos medios para almacenar masivamente información, o al menos lo que se consideraba masivo en aquellos tiempos. Sin embargo, rápidamente se consolidó como una de los medios mas populares, discos de plástico de lectura óptica. El formato fue evolucionando hasta que finalmente fue desbancado por los soportes de memoria virtual ligados al cifrado personal en sus diversos estados, que permitieron finalmente separar la información del soporte físico.

Se encontraba con un doble problema, conocer en cual de los diversos formatos se había grabado la información y después encontrar en alguna tienda de anticuarios una interfaz adecuada para poder leerlos. Su abuelo había sido previsor y diligente, había incluido algunas notas manuscritas en soporte standard de larga duración y casi todos los discos o como mínimo los paquetes principales tenían la fecha registrada manualmente con algún tipo de marcador, que en aquella época se denominaba tinta, que había resistido el paso del tiempo.

En un primer intento pensó que las notas manuscritas le serian de mas ayuda pero ante su impotencia descubrió que prácticamente no entendía nada o era información que carecía ya de sentido. Por un lado no sabia lo que era un CDROM ni que tipo de formato era el DVD. Por otro las indicaciones de que en tal dirección se podía encontrar un reparador de lectores de DVD de doble densidad, tampoco le servían de nada ya que en la susodicha dirección recordaba perfectamente que hacia lo menos veinte años había un enorme complejo lúdico y de animación para personas de segunda juventud, o sea los que tenían entre sesenta y ochenta años.

De mucha mas utilidad le resultaron las fechas. Con estas hizo una búsqueda selectiva en la red standard utilizando el viejo TRASH, heredero de toda una generación de buscadores de red que aparecieron después de que los clásicos buscadores que surgieron después del colapso de GOOGLE y que todavía podía utilizarse en algunos lugares. Después de un par de tentativas para que la red aprendiera que es lo que buscaba, dejó que hiciera el informe solo y que se lo presentara cuando estuviera listo. De todas formas como no le dio prioridad sobre las tareas standard ni a las de su trabajo normal, la pantalla con la información no apareció en el rincón de la pared de su espacio de trabajo, hasta una semana mas tarde. El sistema realmente estaba agobiado no con la información a manejar, sino con las ordenes contradictorias que Junior III le había estado dando últimamente y probablemente también un poco confundido con las contraórdenes que su mujer había dado ya que era una de las pocos personas que había delegado a su esposa poderes totales en la red.

DURANTE EL PRIMER TERCIO DEL SIGLO XXI SE HABÍAN UTILIZADO AMPLIAMENTE DIVERSOS MEDIOS PARA ALMACENAR MASIVAMENTE INFORMACIÓN, O AL MENOS LO QUE SE CONSIDERABA MASIVO EN AQUELLOS TIEMPOS

El sistema informático había hecho un buen trabajo, aunque algo sorprendido, nos referimos al sistema automático de búsqueda, incluyó una nota aclarando que toda la información era fiable pero declinaban toda responsabilidad sobre las consecuencias de la utilización de la misma en la fabricación de elementos que supusieran el almacenamiento de información. Años de abogados sabelotodos y estériles pleitos, habían acostumbrado a todo ente fuera físico o virtual

a cubrirse las espaldas ante cualquier reclamación. Por lo visto el software había interpretado su petición como un intento de fabricarse él mismo un equipo para guardar sus datos privados. Nada mas lejos de sus intenciones. Tan solo deseaba conocer que tipo de formato se había empleado para registrar el soporte y resultó que una gran cantidad de ellos eran CD-ROM registrables multispeed de 800 MB de capacidad.

Junior III quedo un poco sorprendido de la escasísima capacidad de aquellos antiguos soportes, aunque ya tenia alguna referencia, no es lo mismo oír en una conversación que ",... a principios de siglo, para almacenar imágenes en movimiento tenían que ocupar un espacio físico enorme en su propia casa..." que tener en sus manos un pesado disco de plástico que según la referencia apenas contenía unos cuantos miles de paginas de información. De todas formas la aventura no había mas que empezado. Después tuvo que encontrar un aparato que emulara lo que hacían los antiguos dispositivos. Gracias a la fiebre coleccionista que había estallado hacia los años treinta, se podían encontrar originales, pero eran piezas de coleccionista totalmente fuera de sus posibilidades. Sin embargo los emuladores eran mucho mas asequibles y ademas se evitaba toda la parafernalia de los dispositivos intermedios entre la antigualla y los sistemas actuales de visualización y almacenamiento.

Finalmente lo consiguió. Introdujo uno de los discos en el emulador y tras unos instantes de incertidumbre, sobre la resbaladiza proyección que aquel día parecía particularmente nerviosa y pretendía esconderse detrás de uno de los elementos de decoración, vio una lista de caracteres. Su sorpresa fue mayúscula al no encontrar un volumen organizado de información como estaba habituado. Tuvo que invertir una semana de trabajo esporádico de búsqueda para descifrar el significado. Según parecía en aquel tiempo todo se almacenaba con poco orden identificándose cada elemento de información por una serie de caracteres que encima podían tener distinto significado según el tipo de ordenador que se utilizase. Llegado a este punto le costó menos llegar a la conclusión que todo el disco de plástico no contenía otra cosa que datos de texto escritos mediante un programa llamado OpenOffice. De nuevo buscó y encontró el emulador adecuado y fue entonces cuando realmente vio la serie de documentos redactados probablemente por su abuelo. Al azar dio orden de ampliar y mostrar frente a su mesa de trabajo uno de ellos. Este era su contenido.

EL DESAFIO

Todo empezó por un desafío lanzado frente a una maquina de café. Fue del estilo "...a que no eres capaz de...". Mas vale tener la cabeza fría ante semejantes lances. Sabes como empiezas, pero no como terminas. El desafío era bastante sencillo. Hacerse con la palabra de paso del pobre hombre que, agobiado, se ocupaba en solventar los problemas ofimáticos que todos los días ocurrían en el edificio. Contexto: una empresa de servicios que trabajaba para terceros. Apostantes: empleados de la empresa cliente que no tenían nada mejor que hacer que zanganear frente a la maquina de café.

El desafío tenia sus pequeños detalles. No se podía instalar keylogers ni destrozar el software de las maquinas que pertenecían a la empresa de servicios. Mas

EL DESAFÍO ERA BASTANTE SENCILLO. HACERSE CON LA PALABRA DE PASO DEL POBRE HOMBRE QUE, AGOBIADO, SE OCUPABA EN SOLVENTAR LOS PROBLEMAS OFIMÁTICOS QUE TODOS LOS DÍAS OCURRÍAN EN EL EDIFICIO

que nada porque nadie quería perder el empleo. Una cosa eran las apuestas y otra el dinero que cada mes se ingresaba en la cuenta bancaria. Mientras volvía a la mesa donde transcurrían las largas horas de trabajo, medité sobre las diferentes posibilidades. La red estaba compuesta por maquinas bastante homogéneas de la familia Windows, algunas eran Windows 2000 y otras XP, todavía no había ninguna VISTA instalada. Lo mas sencillo era arrancar un PC de la empresa que les hospedaba desde una distribución mínima linux y copiar alguno de los ficheros de la SAM, o bien podía intentarse sacar la hash que estaban en el cache con cachedump.

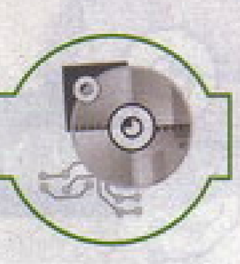
La segunda opción era la mas atrayente y en teoría mas fácil, tenia un CD lleno con diversas utilidades entre ellas ésta pero se encontró con la dificultad que el antivirus corporativos detectaba cachedump como un virus y lo ponía automáticamente en cuarentena. Podía intentar desactivar el antivirus, pero esto podía infringir una de las reglas del desafío si se las interpretaba de forma estricta. Tenia a su disposición la distribución Dam Small Linux (http://www.damnsmalllinux.org) que cabía en su llave USB, pero con ella aunque podía montar el disco duro donde residía el Windows y copiar los archivos que le fueran necesarios, después no tenia las herramientas necesarias para tratar los datos. Tenia que bajárselas de Internet y después instalarlas en algún sitio y esto infringía otra de las reglas del juego y ademas no tenia muchas ganas de perder tiempo.

Sabiendo que la empresa tenia una de las salas de reuniones provistas con servicio wifi restringidos solo para visitas de cierto nivel, pensó que con un poco de suerte la solución estaba en romper la clave del servicio wifi y ver si le daba alguna pista sobre la password del pobre supervisor que probablemente ya debía estar bastante falto de recursos como para perder tiempo inventándose nuevas. Si el cifrado era WEP no debía darles demasiados problemas, alguna distribución diseñada para encontrar agujeros de seguridad le podía facilitar el trabajo al tener ya instaladas todas las utilidades que le hicieran falta. Una vuelta por la red le dio varias posibilidades, una de ellas era BackTrack V2.0 (http://www.remote-exploit.org/backtrack.html)

BackTrack V2.0

BackTrack es una distribución linux resultado de la herencia de SLAX. Se presenta bajo la forma de una distribución LiveDistro, o sea arranca directamente desde un CD y no hace falta instalar nada desde el disco duro, por tanto no deja apenas traza de lo que se ha hecho y con un poco de suerte ni siquiera quien lo ha hecho. SLAX (http://www.slax.org) es una distribución que nació en un principio



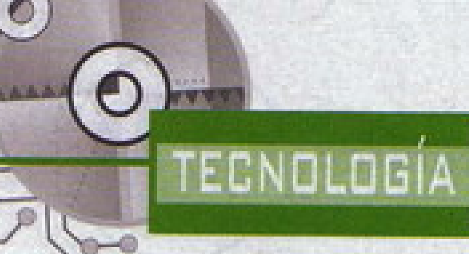


con la voluntad de crear una LiveDistro que fuera fácilmente modificable y ajustable a las necesidad especificas de cada uno. Basada en Slackware tiene una herramienta especifica que permite con gran soltura añadir, eliminar o modificar la composición de la distribución de base, llamada "MySLAX Creator". Fue con estas herramientas que los impulsores del proyecto configuraron BackTrack.

Las primeras versiones se orientaron con la filosofía "contra mas programas mejor", lo cual no es siempre una buena idea. Después cambiaron de ideas y se focalizaron en conseguir estabilidad, cohesión y orden. La ultima versión esta bien estructurada aunque padece de escasa capacidad en detectar hardware esotérico, aunque es bastante lógico. El objetivo del esfuerzo de sus creadores no es que el primer imberbe provisto con el laptop que le han regalado sus papas ataque el ordenador del vecino, que nunca se ha metido ni con él ni con su familia, sino que un profesional pueda realizar test de seguridad de una forma cómoda.

La organización del menú sigue la lógica de cualquier investigación sobre seguridad informática y los programas están agrupados bajo los epígrafes de "Enumeración", "Explotación de archivos", "Scanners", Ataque a passwords", Fuzzers", "Spoofing", Sniffers", "Tunneling", Herramientas para Wifi", "Bluetooth, "Herramientas contra Cisco", "Herramientas para bases de datos", "Análisis forense", "Servicios" y "Ingeniería inversa". Bajo todo eso se almacenan mas de 300 herramientas que debieran ser mas que suficientes para conseguir sacar partido de una red con protección media que son las que mas abundan dentro de las que se consideran como seguras.

Dentro de cada menú hay desde las herramientas mas conocidas hasta las mas extrañas y también algunas banales e incluso inútiles. Como muestra de la colección se destacan utilidades del tipo de PIRANA que intentan ataques a servidores SMTP y evalúan la posibilidad de circunvalar los filtros de seguridad, NETDISCOVER que determina la topologia de una red de forma pasiva, NMAP que no necesita presentación, NITKO que escanea vulnerábilidades en servidores web, HYDRA que en base a un diccionario determina las password poco seguridad en múltiples servicios para un mismo servidor, JOHN THE RIPPER en su ultima versión y con todos los parches, WIRESHARCK heredero de ETHEREAL famoso y prodigioso analizador de protocolos, AIRCRACK diseñado para romper password



WEP y WPA-PSK, AIRSNORT con el mismo objetivo y un largo etcétera. Material mas que suficiente para cualquier ataque en regla.

DETECTANDO EL HARDWARE

Ni corto ni perezoso me bajé la distribución y quemé un CD con su contenido. Tenia a mi disposición un PC portátil de nueva generación apenas entregado con todas los dispositivos de seguridad al uso. Tuve un momento de pánico cuando intenté arrancar desde el CD ya que algunos administradores tratan, con muy buen criterio, de evitar que los usuarios utilicen otros OS que no sean los corporativos, pero en este caso suavemente arrancó a la primera. Uno de los primeros problemas con que uno se enfrenta al utilizar una distribución linux LiveCD, es la detección del hardware. Casi nunca hay problemas con teclado y ratones, algunas veces no detectan los nuevos discos de los últimos laptop, muchas veces ignoran los periféricos USB y a menudo se niegan a trabajar con las tarjetas wifi integradas. En mi caso me encontré con que la Intel PRO/Wireless 3945ABG integrada en la placa base era totalmente ignorada.

Sin un dispositivo capaz de analizar y espiar la red era totalmente inútil toda la parafernalia que había montado, así que había que encontrar una solución que se adaptara a mis necesidades. Habían distintas posibilidades, una de ellas era simplemente comprar una maquina que reuniera los requisitos precisos. Tiempo tenia, dinero también. Primero me aseguré que lo que compraba iba a ser reconocido por BackTrack, para ello me dirigí a la pagina http://backtrack.offensive-security.com/index.php?title=HCL:Wireless#Wireless_Cards_And_Drivers , donde con suficientes detalles hay información para asegurar la compra. Después me acerqué a e-bay (http://www.ebay.es), para buscar lo que se ajustara a mis exigencias. Ebay.es, o sea la versión de e-bay dedicada al mundo de habla hispánica, no hace mucho que funciona pero es bastante efectivo, sino se buscan cosas demasiado raras y no se esta convencido que se pueden encontrar duros a cuatro pesetas, o sea que el precio del articulo se ajuste a la calidad del producto. No voy a dar una lección de como comprar en este sitio, cada uno es libre de aprender como pueda y nada como la experiencia para hacer sabios en cualquier tema, aunque aconsejo empezar comprando cosas por un valor máximo de diez euros.. El caso es que se pueden encontrar equipos por menos de 200€ en eBay, gastos de transporte y embalaje incluidos. Era otro de los motivos para utilizar los servicios de e-bay.es, pues al ser el mercado mas local los gastos de transportes son inferiores y con un poco de suerte nulos si el vendedor vive en la misma ciudad. Casi estaba decidido a pujar cuando se me ocurrió leer atentamente la lista del hardware que era reconocido por BackTrack. No puedo insistir bastante que leer, atentamente , es madre de todos los sabios y padre de las personas inteligentes. Ahí se decía que el chipset ACX100 tenia soporte bajo BackTrack siempre que se cumplieran ciertas condiciones.

Revolviendo en mi maleta mágica, descubrí que con mi persona viajaba desde hacia tiempo una USRobotics 5410 y si no recordaba mal, estaba construida con un chipset de Texas Instrument ACX111. No era lo mismo que un ACX100 y toda la documentación afirmaba que había que tener cuidado, pero yo no tenia nada que perder, así que la desenterré de las profundidades de mi maletín y la conecté al nuevo laptop. El arranque fue un poco decepcionante, la pequeña lucecita de la tarjeta estaba muy poco animada, clara prueba que no era detectada, pero buscando un poco en el menú, descubrí un "Load ACX100" bajo el menú "BackTrack" ==> "Radio Network Analisys" ==> "80211" ==> "Misc", bastante indicativo. Pulsar sobre el botón e iluminarse el led rojo de la tarjeta fue todo uno. El resto de la historia tenia que ser mucho mas fácil. Bajo el mismo menú se encuentra kismet, que los chicos de BackTrack han tenido la delicadeza de implementar de forma autoconfigurable con lo cual me ahorré el tener que modificar a mano el fichero de configuración. Es suficiente con clickear sobre el menú desplegable para que se abra una sesión y empiece a rastrear la red.

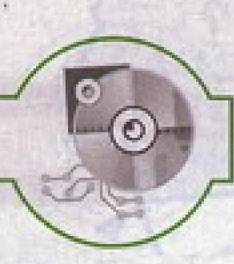
EL DESAFÍO ERA BASTANTE SENCILLO. HACERSE CON LA PALABRA DE PASO DEL POBRE HOMBRE QUE, AGOBIADO, SE OCUPABA EN SOLVENTAR LOS PROBLEMAS OFIMÁTICOS QUE TODOS LOS DÍAS OCURRÍAN EN EL EDIFICIO

La red corporativa y algunos laptop no declarados aparecieron en la pantalla junto a las estadísticas de cada emisor y los datos principales. Tomé nota de la que me interesaba y las anoté cuidadosamente. A continuación me dediqué a jugar con Aircrack, herramienta, que todo hay que confesar si se quiere tener la conciencia tranquila, nunca había utilizado, pero es que el propio BackTrack suministra la documentación necesaria con un simple "man aircrack-ng" Lo demás fue solo cuestión de paciencia y encontrar el momento adecuado y la tranquilidad necesaria. Había que encontrar el momento para situarse cerca de la sala de reunión y esperar a que hubiera suficiente trafico. Tampoco fue cosa de cinco minutos pero el cabo de una semana había conseguido la clave WEP. Los administradores de la red no se habían complicado la vida y no habían implementado nada mas serio que un simple cifrado WEP.

ATAQUE DEFINTIVO

La famosa clave estaba compuesta por una palabra común del diccionario de la lengua en que me encontraba, seguida por un símbolo no ASCII y después dos dígitos que representaban el año en curso. Deduje que habían tomado una palabra fácil de recordar, después habían añadido un carácter que ellos consideraban imposible de deducir y a continuación cambian la clave cada año a base de seguir la fecha en curso. Difícil de descubrir si no se dispone de ninguna pista, ya que la palabra no tenia ninguna conexión con la corporación, pero fácil de deducir si se conoce la regla.

Quedaba por encontrar la password del administrador, que fue quien me metió en este desafío. Habían diversas posibilidades. Una de ellas, la mas fácil, es que hubiera elegido exactamente la misma. Una pequeña prueba le demostró que estaba equivocado. Otra posibilidad es que hubiera utilizado mezcla de mayúsculas y minúsculas, pero la deshecho ya que resulta mas difícil de recordar de lo que parece a primera vista. Otra posibilidad es que



hubiera tomado el siguiente carácter especial que se encuentra en el teclado a continuación del que tomó para la clave WEP. Ahí acerté plenamente. Encontrada, la password, ganada la apuesta. Semanas mas tarde tuve que lamentar esta historia, ya que se corrió la voz y tuve que dar explicaciones. Esto me enseñó que los únicos secretos que se guardan son los que solo uno mismo conoce y que hay cierta fama que no aporta ningún beneficio. Consejo para mis posibles lectores. Sed sumamente prudentes.

ALGO MÁS SOBRE BACKTRACK

Es esta ciertamente una distribución de calidad y que no se limita a compilar algo existente. Vale la pena invertir tiempo en descubrir lo que esconde. Una de sus peculiaridades, implementación semiautomática de ACX100 y configuración automática de KISMET, ya la he contado, pero es que tiene muchas mas cosas y una de ellas es la posibilidad de implementar CLUSTERS de maquinas para lanzar John the Ripper de forma que participen de forma conjunta en una sesión de crack.

La aplicación practica de la configuración propuesta es mas que limitada ya que se requiere, disponer de toda un subredes propias y que no haya ningún server DHCP en ella. Esta hipótesis solo se presenta en la practica en las salas donde se imparten cursos de informática o similares, de todas formas si hay entre los que me leen algún alumno con tiempo libre y disponibilidad de la llave de la aula, puede probar suerte. Primero hay que arrancar que hará de servidor con los siguientes argumentos "server|pxe|john-mpi", asignar un nombre para el cluster y una palabra de paso. Después se arrancan el resto de las maquinas como clientes con la opción "client|john-mpi". Las maquinas clientes van pidiendo el nombre del servidor y la password. Hay que copiar la hash en cada cliente, ya que la versión que probé no lo hacia desde el servidor. A continuación los clientes entran en el cluster contribuyendo al calculo general.

La adición de un nuevo paquete también es bastante sencilla. En la practica basta con crear el directorio donde se quiere hacer la compilación, teclear ".:configure && make" y después lanzar "checkinstall", se generara un archivo con extension "tgz" que hay que convertir en "mo" mediante "tgz2mo" Uno puede guardarse para si mismo el regalo o bien mandárselo al equipo que se encarga de mantener la distribución oficial. Su dirección es muts@remote-exploi.org

REFLEXIONES

Sin que lo advirtiera, la luz de la estancia se había atenuado y la pantalla virtual se había acercado y aumentado su luminosidad. El sistema inteligente de control de bienestar del hogar había detectado que la lectura le había interesado y se esforzaba en facilitar su entorno. Viajero Junior III estaba un poco sorprendido de la lectura del documento. Gran parte de la descripción técnica de las notas que acaba de leer le sonaban totalmente a sánscrito, pero lo que era evidente es que el pasado se cruzaba con su presente. Se prometió arrancar tiempo a sus actividades programadas para continuar descubriendo los archivos secretos de su antepasado. Nosotros también prometemos relatar lo que encuentre. A veces las promesas se cumplen....

2007 SET, Saqueadores EdicionesTécnicas.
Información libre para gente libre
www.set-ezine.org
web@set-ezine.org





TRUCOS ANTIDEBUGGING

Parte III

Bienvenidos una vez más al mundo del cracking, donde el antidebugging es rey. :) Hoy veremos más trucos interesantes, algunos más utilizados que otros, pero no menos importantes por ello. Veamos que podemos descubrir, acompañenme.

Trucos anteriores

Antidebugging utilizando SEH, el cuál es bastante interesante, ya que genera una excepción, donde en debuggers como Olly, produce que se termine el proceso inesperadamente, lo cuál dificulta el debuggeo de la aplicación.

```
_SehExit:
  POP FS:[0]
  ADD ESP,4
  JMP _Exit

end start
```

Finalmente, la rutina de aquí arriba, funciona para poder salir de la excepción generada por el sistema, al no encontrar el debugger. Es decir, el SEH.

Vemos que al principio de esta rutina, se hace un push, de la dirección que pertenece a la etiqueta _SehExit. Al terminar, se recupera esa dirección, se suma 4 a ESP, y luego se redirecciona a la etiqueta Exit, para salir finalmente.

Una extensión de la característica NtGlobalFlag, podemos verlo aquí, este trozo de código es utilizado por el conocido protector ExeCryptor.

```
1.ASSUME FS:NOTHING
2.MOV EAX,DWORD PTR FS:[30h]
3.ADD EAX,68h
4.MOV EAX,DWORD PTR DS:[EAX]
5.CMP EAX,70h
6.JE @DebuggerDetected
```

Ya hemos visto algo similar antes, pero aquí lo vemos directamente del protector mencionado. Veremos que nos vamos hacia el offset 68h, como marca la línea 3.

Por último obtenemos ese byte, de esa posición, y se compara con el valor 70h, si tiene ese valor, es porque los FLAGS me mecioné anteriormente fueron seteados, sino, no. :)

Sexto Ejemplo

En el último ejemplo de antidebugging, que veremos en este número, es uno de los más conocidos, denominado RDTSC.

```
RDTSC
XOR ECX,ECX
ADD ECX,EAX
RDTSC
```

Este truco, simplemente, mide por tiempo, la ejecución, entre dos marcas RDTSC. Si lleva más de lo esperado, puede haber un debugger en el medio, que esté interceptando las instrucciones más importantes.

```
SUB EAX,ECX
CMP EAX,0FFFh
JNB @OllyDetected
```

El tiempo es devuelto en el registro EAX, y por lo tanto, si el valor devuelto es mayor que FFFh, entonces, hay un debugger en el medio.

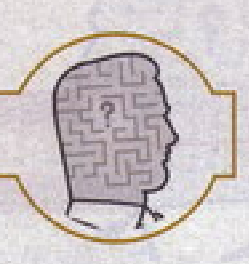
Detección por TLS Callback

La detección de un debugger por TLS, debe ser explicado por lo que es primero TLS.

TLS significa Thread Local Storage, y es un espacio estático o dinámico de memoria, asignado para un thread (hilo).

El TLS, pertenece a la estructura del PE, y es ni más ni menos que parte de un PE. Lo cuál eso hace incidir sobre los debuggers. ¿ de qué forma ?

Cuando un debugger carga un PE en memoria, antes de analizar la sección de código, analiza lo que sucede en la sección TLS. Si en TLS combinamos a la detección de la API IsDebuggerPresent, podremos detectar el debugger, antes de



que sea visto siquiera el código desensamblado del programa.

Este código de aquí abajo hace que la aplicación salga.

```
PUSH 0
CALL ExitProcess
RET
```

Este código de aquí abajo, se ejecuta antes que la sesión de código.

```
TLS:
; TLSCalled flag indicates that TLS is
called only once on application
; initialization. It can be called on
application exit again. This switch
; disables that.

CMP BYTE PTR[TLSCalled],1
JE @exit
MOV BYTE PTR[TLSCalled],1
CALL IsDebuggerPresent
```

Veremos la variable TLSCalled, es utilizada como switch, cuando la aplicación se inicializa. Entonces compara, si la variable, ya vale 1, sale del programa, sino activa la variable, y chequea con la API IsDebuggerPresent si un debugger está analizando el programa.

```
CMP EAX,1
JE @DebuggerDetected
```

En el caso de que sea detectado, se muestra un mensaje, en el caso negativo, el programa termina exitosamente.

Si debuggeamos la aplicación de ejemplo, veremos que el debugger Olly por ejemplo, muestra un mensaje de "Debugger detected!", lo cuál significa, que el código en TLS se ejecuta antes.

Si vemos en el entrypoint del fichero, no encontraremos el código de detección, sino que después de que el programa termina, veremos la rutina, la cuál es parcheable obviamente. Pero imaginemos, que en lugar de mostrar un cartel, cierre un debugger automáticamente.

Esto lo veremos en el EOP del fichero:

```
00401000            PUSH 0
00401002            CALL <JMP.&kernel32.
ExitProcess>
00401007            RETN
```

Con lo cúal puede complicar el análisis para un novato. Imaginemos que también puede darse la situación, que incluyamos una VM en el fichero, lo cual, cuando sea detectado el debugger, no sería a través de código simple, sino a través de una maraña de código de una máquina virtual, con código interpretado.

Ahí se haría el chequeo por el debugger. Complicaría bastante el análisis, ¿ no creen ?

Truco de detección Anti OEP Generic

Herramientas como Peld, tiene plugins para detectar el EntryPoint (OEP) de los ejecutables, de manera de poder encontrar su inicio fácilmente.

HERRAMIENTAS COMO PEID, TIENE PLUGINS PARA DETECTAR EL ENTRYPOINT (OEP) DE LOS EJECUTABLES, DE MANERA DE PODER ENCONTRAR SU INICIO FÁCILMENTE

Resulta, que los programas empacados, tienen dos o más EOP. Uno de la aplicación empaquetada, o de lo que se podría decir el "envoltorio" o stub, y otro de la aplicación principal.

Estos plugins lo que hacen, es ejecutar el programa en memoria, esperar que se desempaquete, y luego buscar en lazona de memoria reservada para ese proceso, el OEP original de la aplicación.

Esto lo hacen, buscando por patrones de OEP genéricos, por compilador. Cada compilador genera OEP similares, pero con distintas instrucciones, u orden de instrucciones.

El truco consiste, en inyectar un OEP falso, dentro de la zona de memoria reservada para nuestro proceso, de manera que se encuentre un OEP falso, y hasta se informe de que se utilizó un compilador que no fué el original, por ejemplo, Visual C++.

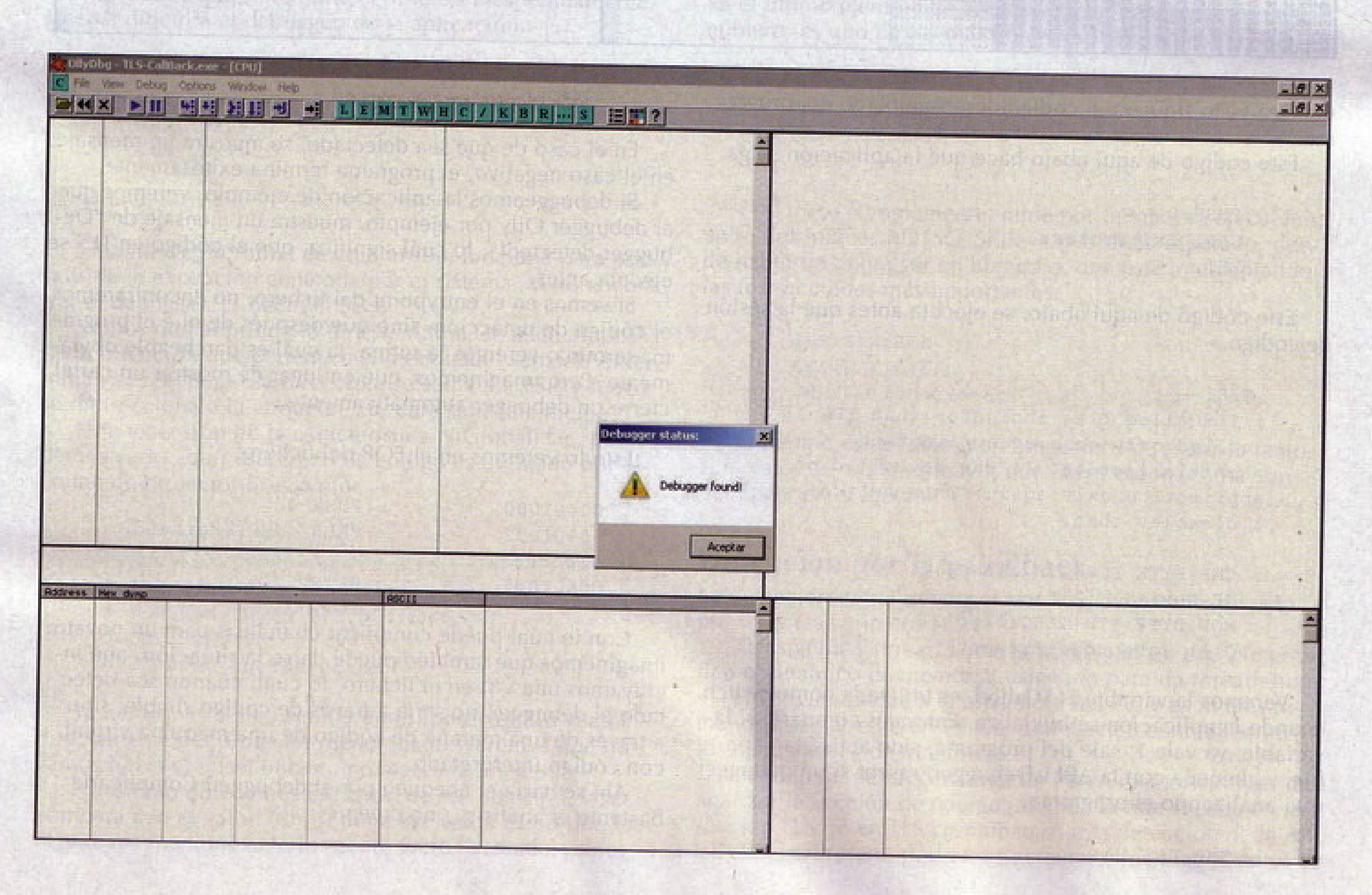
El código de este truco es bastante simple, veamos de qué se trata.

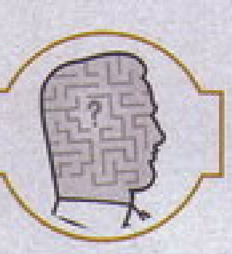
Antes de proceder con el truco, deberemos modificar el OEP del fichero hacia por ejemplo 401030h.

El falso OEP, estará en 401000, en este ejemplo.

```
    AntiGenOEP      db 55h,8Bh,0ECh,6Ah,0FFh,68h,0F8h,40h,40h,0
0h,68h,0F4h
                    db 1Dh,40h,00h,64h,0A1h,00,00,00,00,50h,64h
,89h,25h,00
                    db 00,00,00,83h,0ECh,58h,53h,56h,57h,89h,65
h,0E8h,0FFh
                    db 15h,58h,40h,40h,00,33h,0D2h,8Ah,0D4h
```

Como podemos ver aquí arriba, se trata de un OEP, de los que genera Visual C++. Obviamente, éste es el OEP falso, que inyectamos en 401000.





```
View - CheckRemoteDebuggerPresent.asm
File  Edit  View  Help
;       FALSE value if debugger is present in selected process.

;       Load the function via GetProcAddress

        PUSH offset krnl                ;kernel32.dll
        CALL LoadLibrary

        PUSH offset chkrdbg             ;CheckRemoteDebuggerPresent
        PUSH EAX
        CALL GetProcAddress

;       IsItPresent variable will store the resault

        PUSH offset IsItPresent
        PUSH -1
        CALL EAX

        MOV EAX,DWORD PTR[IsItPresent]
        TEST EAX,EAX
        JNE @DebuggerDetected

        PUSH 40h
        PUSH offset DbgNotFoundTitle
        PUSH offset DbgNotFoundText
        PUSH 0
        CALL MessageBox

        JMP @exit
  @DebuggerDetected:

        PUSH 30h
        PUSH offset DbgFoundTitle
1.606 bytes                                    Windows text
```

```
        PUSH 40h
        PUSH offset MsgTitle
        PUSH offset MsgText
        PUSH 0
        CALL MessageBox
        RET
```

Este código de aquí arriba, está para rellenar de algo el programa principal, simplemente muestra un cartel, pero no es el fin del programa detectar un debugger, sino complicar a los plugins de búsqueda de OEP genéricos.

Anti RDG Detection

Para los que no conocen que es RDG Packer Detector, se trata de un detector de empaquetadores, crypters y compiladores.

Esta programado por un amigo argentino RDG, bastante interesado en detectar mi protector Uranium Protector, a propósito, si estás leyendo esto RDG, te mando un saludo. :)

Lo que hace RDG, es chequear en el OEP por patrones. Si concuerda con algún patrón en el ejecutable o en la base de patrones en el archivo de texto, mostrará el nombre del protector, empaquetador o compilador que fué detectado.

Entonces, podemos hacer similar a como hicimos en el truco anterior, insertar una cantidad de bytes, en el OEP y provocar que detecte un protector erróneo.

Este es el OEP típica de una aplicación protegida con ASProtect:

```
        PUSH offset @RealStart
        CALL @delta
        RET
        @delta:
        RET

      ; Bytes basura, no tienen un significado.

        db 0Bh,0B6h,66h,0B1h,22h,0B7h
```

Ahora veremos como se compila este código de aquí arriba:

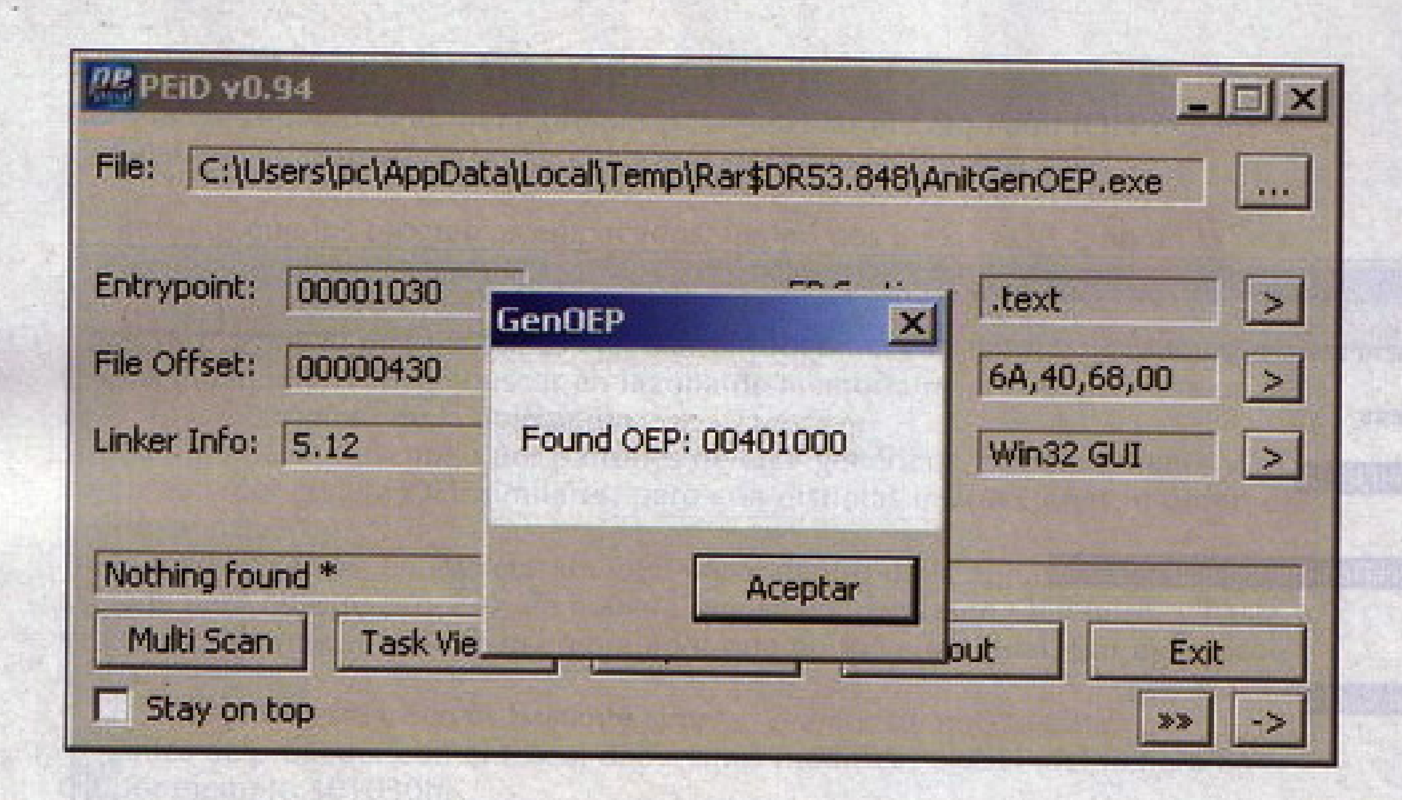
```
00401000      PUSH AntiRDG-.00401012
00401005      CALL AntiRDG-.0040100B
0040100A     RETN
0040100B     RETN
```

Veremos ahora como es en binario este código:

```
68 12 10 40 00 E8 01 00 00 00 C3 C3
```

Este de aquí arriba, como podemos ver, es el OEP típico de ASProtect.Sería lo que nuestro querido RDG Packer Detector buscaría. :)

```
        @RealStart:
        PUSH 40h
        PUSH offset msgTitle
```




```
PUSH offset msgText
PUSH 0
CALL MessageBox

PUSH 0
CALL ExitProcess
```

Aquí arriba es donde empieza el verdadero EOP, como veremos, seguramente RDG, detectará ASProtector, cuando nuestro programa no está protegido con éste protector, ni con ningún otro.

Aunque debo decir que las versiones más nuevas de éste detector, ya detectan las signaturas o OEP falsos.

Detección por mala formación de strings

Este truco, aprovecha un error del debugger Olly, para romperlo. Utilizando un nombre de archivo del tipo %s%s, provoca que Olly se rompa, y no pueda ser debuggeado con este.

```
    PUSH 512
    PUSH offset filename
;%s%s.exe
    PUSH 0
    CALL GetModuleFileName

    MOV ECX,offset filename
    ADD ECX,EAX
```

Aquí obtiene el nombre del archivo. Y lo carga en memoria.

Luego hay una iteración hasta encontrar el símbolo '\'. Si lo encuentra, significa, que encontramos el nombre del archivo.

```
    PUSH ECX
    PUSH offset
OriginalFileName    ;%s%s.exe
    CALL lstrcmp
```

Ahora que obtuvimos el nombre del archivo, lo comparamos con el patrón '%s%s.exe'.

```
TEST EAX,EAX
JNE @DebuggerDetected
```

Si no son iguales se detectó el debugger. Si son iguales entonces continuamos la ejecución de manera correcta y normal.

Conclusión

Bien amigos, hemos visto algunos trucos más, lo cuál podemos estudiar de mejor manera con pruebas, mejoras, mezclando trucos, insertándolos en crackmes, y en nuestras propias protecciones.

Seguirán saliendo trucos, y métodos de dificultar el análisis, eso siempre será así, ya que el software de análisis binario, siempre está sujeto a errores, e inclusive, podemos armar una trampa, para que al ser debuggeado, se aproveche un error para infectar la máquina del analista en seguridad.

Espero que les haya gustado.

Nos vemos la próxima.

SparK

arielrm@intrabytes.com
spark@disidents.org
www.intrabytes.com
www.disidents.org

ESTE TRUCO, APROVECHA UN ERROR DEL DEBUGGER OLLY, PARA ROMPERLO



truecrypt

Criptografía avanzada que podría usar tu prima pequeña

Un joven hacker escucha música demasiado alta mientras teclea furiosamente en el teclado de su ordenador portátil. En una memoria USB conectada a su equipo guarda toda su información privada, datos que preferiría que nadie viera, algunos incluso que podrían resultar comprometedores. A pesar de ello, lleva siempre la memoria encima, sin temor a perderla o que se la roben. Sabe que, aún en el caso de que alguien se hiciera con la unidad, identificara el carácter cifrado de los datos, y fuera capaz de realizar un ataque de fuerza bruta para obtener la contraseña; sólo vería un archivo de texto con tres únicos caracteres escritos en él, una sonrisa sardónica que saludaría desdeñosa al hipotético ladrón. ¿Ciencia ficción? ¿Película de Hollywood? Ni mucho menos... :-)

Hola una vez más, y sed todos bienvenidos, apreciados lectores. En el artículo que tienes entre las manos, vamos a hablar de uno de los mejores programas de seguridad que he podido ver en los últimos años: TrueCrypt. La situación descrita en la introducción del texto es, obviamente, una "licencia literaria", pero podría perfectamente ser posible gracias a este software de cifrado. ¿Cómo? Sigue leyendo...

Datos por doquier

Hace muchos años, el almacenamiento de información en soporte digital era algo reservado para importantes empresas o gobiernos, siendo el uso de estas tecnologías por parte de los usuarios de a pie algo meramente anecdótico. Tampoco eran muchos los usuarios de ordenadores que deseaban tener datos almacenados de forma persistente y segura, más allá de un puñado de disquetes que se guardaban en un cajón junto a la máquina. Desde esa época de discos duros cuya capacidad se medía en megabytes, hasta la actual en que es algo habitual tener más de un terabyte de almacenamiento en un domicilio cualquiera, las nuevas tecnologías han cambiado mucho.

Ahora los usuarios de ordenadores sí necesitan guardar datos importantes en sus ordenadores. El formatear un equipo y borrar el disco entero ya no es la norma, pues casi cualquier persona debe respaldar antes una gran cantidad de datos que no desea perder. Gracias a los discos externos, muy baratos y de enorme capacidad, ésto no es un problema muy grave.

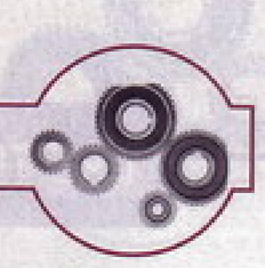
Sin embargo, también las comunicaciones han ido enraizándose poco a poco en nuestras vidas, y seguramente cualquiera de vosotros tendrá decenas de cuentas diferentes en la red: correo, foros, páginas web... la "web 1.0" ha muerto, y actualmente casi todo requiere de una cuenta personal. Si sois medianamente precavidos, cada cuenta tendrá una contraseña diferente; y si no lo sois, por lo menos tendréis tres o cuatro distintas. En cualquier caso, resulta conveniente que esos datos estén almacenados en alguna parte para ser accedidos si, eventualmente, nos olvidamos de ellos; pues aunque nuestro navegador recuerde las contraseñas, nadie está libre de que el sistema operativo sufra una muerte instantánea y asintomática, más aún si sois sufridores -que no usuarios- de Windows.

Guardando secretos

Y por ahí comienzan a venir los problemas: ¿cómo guardar esos datos? La opción del postit en el monitor, o del cuaderno junto al ordenador, es lo primero que viene a la cabeza a quienes no estén muy preocupados por la seguridad. No es mala idea si tu uso del ordenador es doméstico, lúdico o anecdótico. Cuando no es así, comienza a ser habitual el hecho de manejar diariamente varios ordenadores: que si el portátil, que si el sobremesa, que si el del trabajo... y, claro, querrás acceder a todas tus cuentas cuando lo necesites. Aquí es donde la opción del cuaderno comienza a flaquear.

Las memorias USB son una de las mejores herramientas que poseemos las personas que, como antes he comentado, utilizamos varios equipos a lo largo del día. Cada vez más baratas, y con capacidades más que respetables, el problema no es ya llevar un archivo con datos de esta guisa encima, sino en cómo evitar que perder la memoria (algo no muy difícil, pues también son cada vez más pequeñas) suponga exponer nuestros datos. Y es precisamente aquí donde entra en juego la criptografía.

Ya en 1997, un hombre llamado Paul Le Roux pensó en estos problemas, y creó un software de cifrado al vuelo llamado E4M (Encryption for the Masses). Este tipo de programas de cifrado al vuelo (OTFE, del inglés On The Fly Encryption) permiten utilizar volúmenes cifrados virtuales como si de discos físicos se trataran, abstrayendo la complejidad interna de cara al usuario, el cuál sólo realizará las operaciones habituales sobre ficheros, dejando el resto al sistema operativo y al software particular. Lamentablemente (para la comunidad de software libre), Paul Le Roux dejó de de-



sarrollar E4M en el año 2000, cuando comenzó a trabajar en su sucesor comercial, DriveCrypt.

Renaciendo de sus cenizas

Pero no todo acabó ahí, ni muchísimo menos. Cuatro años después del abandono de E4M por parte de Paul, un grupo de desarrolladores utilizó el código para desarrollar un nuevo software llamado TrueCrypt, que continuaría la tarea de su predecesor, y que llegaría a convertirse en uno de los máximos exponentes del software libre aplicado a la criptografía.

El 2 de febrero de 2004 se liberó la primera versión del programa, la 1.0. Sus cambios con respecto a E4M 2.02 eran muchos y muy importantes, a destacar:

- Soporte para Windows XP/2000.
- Protección contra ataques de predicción en volúmenes nuevos, al rellenar la información inicial con datos pseudoaleatorios en lugar de ceros lógicos.
- Protección sector a sector con claves de uso único adicionales.
- Por primera vez en un software libre de cifrado al vuelo para Windows XP, se incluía la característica de la "plausible deniability".

Este concepto de "plausible deniability", que traduciríamos como "denegabilidad creíble", es de gran importancia en el mundo de la criptografía, pese a estar tradicionalmente asociado con temas de espionaje y operaciones secretas. El significado práctico supone la posibilidad de ser capaz de negar algo sin que nadie pueda aportar pruebas en un sentido contrario.

Dado que los ficheros con información cifrada por TrueCrypt no contienen ningún tipo de huella, cabecera o elemento característico en su interior, es imposible distinguirlos de información aleatoria hasta que se han descifrado con la clave correcta. Por ello, es absolutamente imposible demostrar que un fichero contiene datos cifrados sin conocer la clave. Esto supondría únicamente el primer nivel de la "plausible deniability" disponible en TrueCrypt, pues existe un nivel adicional, más avanzado, del que hablaremos un poco más adelante.

El desarrollo avanza

Como nota curiosa, al día siguiente de la liberación de la versión 1.0, se liberó la versión 1.0a eliminando el soporte para sistemas Windows 98/ME. El problema era que el driver usado para dichos sistemas provenía de un intercambio realizado (a cambio del driver para Windows NT) originalmente por los autores de E4M y Scramdisk. Dado que ambos, en el momento de aparición de TrueCrypt, estaban trabajando en DriveCrypt, se denegó el uso del driver y se forzó a eliminar el soporte para los sistemas afectados.

Unos meses más tarde, concretamente el 7 de junio, es liberada la versión 2.0, según parece por un grupo de programadores diferente (debido al cambio de clave de cifrado usada en la firma del paquete). Esta versión se liberó bajo licencia GPL, aunque un par de semanas más tarde, la versión 2.1 volvió a usar la licencia original de E4M para evitar problemas legales. La versión 2.1a, en octubre de 2004, elimina el soporte del algoritmo IDEA para facilitar el uso del software en entornos sin ánimo de lucro, dado que dicho algoritmo aún está sujeto a patentes en varios países.

En diciembre de 2004 se libera la versión 3.0, la cual supone uno de los empujones más importantes de la historia del proyecto, con muchas y muy importantes mejoras, entre las cuales encontramos:

- Soporte para el algoritmo de cifrado Serpent.
- Soporte para el algoritmo de cifrado Twofish.
- Desmontado forzado de volúmenes, incluso con ficheros que estén en uso. Modo "bestia", vamos.
- Soporte para cifrado en cascada.
- Inclusión de volúmenes ocultos en TrueCrypt.

El soporte para cifrado en cascada permite la utilización de múltiples algoritmos de cifrado para un mismo volumen, de tal manera que se apliquen de forma secuencial a la información, teniendo cada uno de los algoritmos su propia clave de cifrado. Así, un atacante que quisiera violar un volumen cifrado con un algoritmo AES, debería atacar la clave aplicada a dicho algoritmo para obtener la información; mientras que a partir de esta versión era posible generar un volumen que estuviera cifrado con, por ejemplo, el algoritmo AES, después Twofish, y finalmente Serpent, haciendo necesario violar las tres claves para obtener la información protegida.

Volúmenes ocultos

Pero, a pesar de que el cifrado en cascada es una de las características más importantes e interesantes de TrueCrypt, palidece en la lista de cambios junto a la más importante de todas: los volúmenes ocultos. Hace un momento, cuando hablábamos de la "plausible deniability", veíamos que TrueCrypt incorpora un primer nivel de dicha medida mediante la imposibilidad de distinguir los datos cifrados de información aleatoria. Los volúmenes cifrados que se introdujeron en la versión 3.0 suponen el segundo nivel de esta medida.

Mediante esta característica, es posible generar un volumen cifrado virtual que actúe de señuelo y que albergue en su interior un segundo volumen con la información verdaderamente protegida. Ambos ocuparán la misma información lógica al estar contenidos en un único fichero (o partición), pero tendrán contraseñas, algoritmos de cifrado y sistemas de ficheros completamente independientes. Cuando se seleccione el fichero para montar el volumen, qué contraseña se proporcione será lo que determine cuál de los dos volúmenes se monte.

El ejemplo típico que suele darse de la utilidad de este tipo de cifrado, es el de alguien que se encuentra bajo una situación de extorsión que le compele a entregar la contraseña de su información cifrada. Proporcionando la contraseña del volumen externo (el señuelo), se descifrará y mostrará información que, aún pudiendo pasar por sensible, no será la que realmente se quería proteger. Hablando en plata, ni un juez, ni el Papa, ni Jack Bauer podrían obtener tu información. Bueno, el último quizá sí... :-P

Continúa el desarrollo

La versión 3.1, en enero de 2005, añadía la posibilidad de ejecutar TrueCrypt en modo "viajero", directamente desde una unidad de almacenamiento y sin instalación previa, así como el montaje en modo de sólo lectura y el montaje como elementos de almacenamiento masivo extraíbles, para evitar la creación de elementos del sistema por parte del sistema operativo.

En noviembre de 2005 se liberó la versión 4.0, con una enorme cantidad de mejoras y añadidos, entre los cuales cabe destacar:

- Protección contra pérdida de datos en volúmenes ocultos.
- Soporte para plataformas de 64 bits.
- Soporte para el sistema operativo GNU/Linux (largamente esperado).
- Soporte completo para ficheros de clave.
- Añadido el algoritmo de hash Whirlpool.
- Añadido soporte para desmontado automático de volúmenes en determinadas condiciones.
- Añadido soporte para realización de acciones automáticas al iniciar sesión.

Una vez más, encontramos mejoras muy, pero que muy interesantes. La opción de utilizar ficheros de clave permite definir, además de una contraseña para un determinado volumen, un fichero que deberá ser proporcionado simultáneamente para poder acceder al él. Por una parte, proporciona la ventaja de tener dos niveles de autenticación en el cifrado; pero también tiene el inconveniente de que perder el fichero ocasiona la imposibilidad de acceder a la información.

Dado que, en este modo, la operación sobre el volumen trabaja con la contraseña y con el valor hash del fichero de clave, lo más normal es utilizar un fichero arbitrario

que pueda ser accedido desde cualquier parte, por ejemplo una imagen alojada en un servidor de Internet. Huelga decir que el fichero no puede cambiar ni lo más mínimo desde su definición como clave, pues el más ligero cambio hará que el valor de hash no coincida y pierda completamente su valor.

Las versiones actuales

La versión 4.1, a finales del mismo mes, introdujo un importante cambio a nivel criptográfico: la sustitución del modo de operación CBC por el LRW, evitando así un fallo que, bajo determinadas circunstancias, podía comprometer la "plausible deniability". Los volúmenes creados en modo CBC seguirían funcionando, pero los que se crearan a partir de entonces lo harían sólo con el modo LRW. No es el momento de entrar en detalles sobre este tema, pues se escapa a los objetivos del presente artículo, así que recomiendo a aquellos interesados en este punto que busquen información por la red.

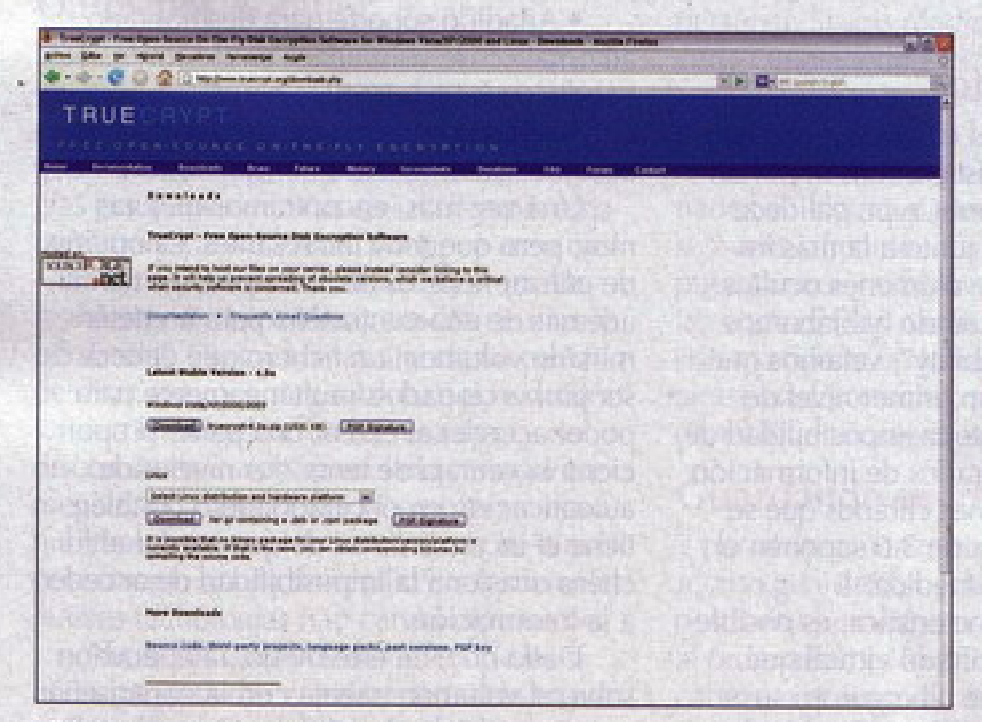
En abril de 2006 se liberó la versión 4.2, que introdujo bastantes mejoras, principalmente en la versión de Linux: posibilidad de crear volúmenes en Linux, uso de ficheros de tamaño dinámico (en sistemas de ficheros NTFS), posibilidad de cambiar las contraseñas o ficheros de clave desde Linux, o uso de múltiples ficheros de clave. La versión 4.2a, en julio del mismo año, no introdujo ninguna mejora o novedad, limitándose a corregir ciertos fallos conocidos.

La versión 4.3 se liberó en marzo de 2007, y añadió, entre otras cosas, soporte para el nuevo sistema operativo de Microsoft (Windows Vista); además de realizar bastantes mejoras y correcciones. La última versión, la 4.3a, fue liberada en mayo de este año, y tampoco incluyó ninguna novedad significativa, aunque sí más mejoras y correcciones de fallos.

Instalando TrueCrypt en Windows

Vamos a comenzar viendo los pasos de instalación para el sistema operativo de Redmond. Lo primero, obviamente, será ir a la página principal del proyecto TrueCrypt (http://www.truecrypt.org/) y acceder a la sección "Downloads". Tras descargar la última versión estable para Windows Vista/XP/2000/2003 -la 4.3a en el momento de escribir estas líneas-, descargaremos también la firma PGP pulsando en el botón "PGP Signature" y comprobaremos su validez:

```
C:\Program Files\GNU\GnuPG>gpg --verify "c:\
Documents and Settings\Ramiro\Desktop\truecrypt-
4.3a.zip.sig"
```



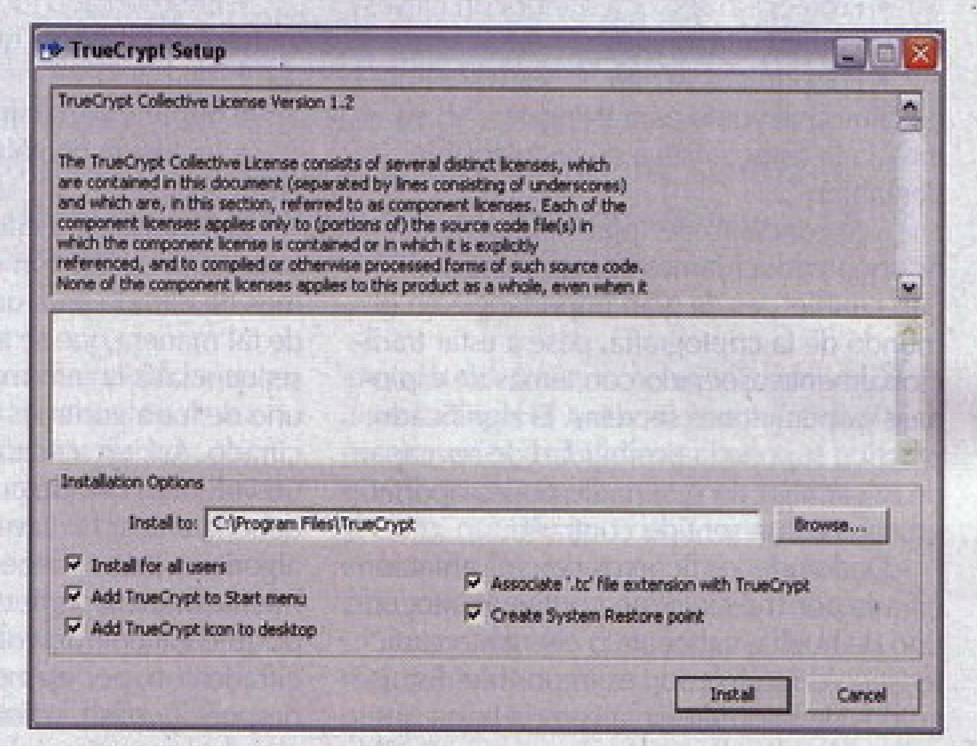
Página de descarga de TrueCrypt.

```
gpg: Firmado el 05/03/07 21:57:18 usando
clave DSA ID F0D6B1E0
gpg: comprobando base de datos de confianza
gpg: 3 dudosa(s) necesarias, 1 completa(s)
necesarias,
modelo de confianza PGP
gpg: nivel: 0  validez:   1  firmada:   1
confianza: 0-, 0q, 0n, 0m, 0f, 1u
gpg: nivel: 1  validez:   1  firmada:   0
confianza: 1-, 0q, 0n, 0m, 0f, 0u
gpg: siguiente comprobación de base de datos
de confianza el: 2007-11-25
gpg: Firma correcta de "TrueCrypt Foundation
```

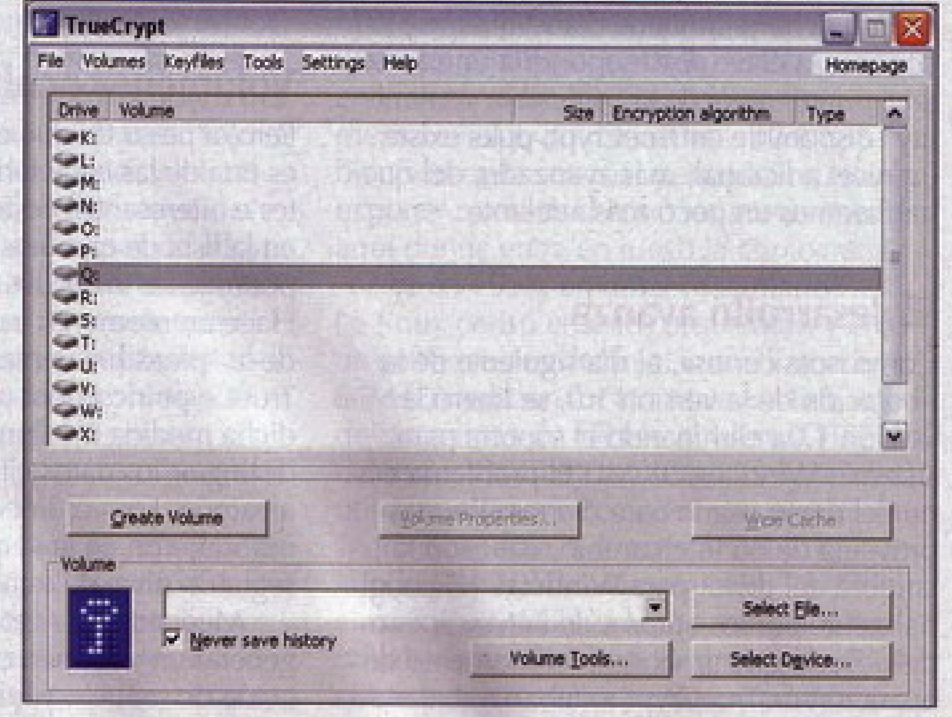
```
C:\Windows\system32\cmd.exe
C:\Program Files\GNU\GnuPG>gpg --verify "c:\Documents and Settings\Ramiro\Desktop\truecrypt-4.3a.zip.sig"
gpg: Firmado el 05/03/07 21:57:18 usando clave DSA ID F0D6B1E0
gpg: comprobando base de datos de confianza
gpg: 3 dudosa(s) necesarias, 1 completa(s) necesarias,
modelo de confianza PGP
gpg: nivel: 0  validez:   1  firmada:   1  confianza: 0-, 0q, 0n, 0m, 0f, 1u
gpg: nivel: 1  validez:   1  firmada:   0  confianza: 1-, 0q, 0n, 0m, 0f, 0u
gpg: siguiente comprobación de base de datos de confianza el: 2007-11-25
gpg: Firma correcta de "TrueCrypt Foundation <contact@truecrypt.org>"

C:\Program Files\GNU\GnuPG>
```

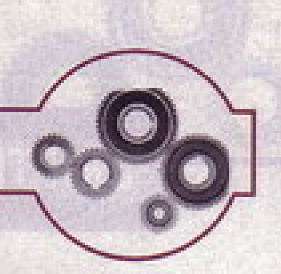
Comprobación de la validez de la firma en Windows.



Instalador de TrueCrypt en Windows.



Ventana principal de la aplicación en Windows.



```
<contact@truecrypt.org>"

   C:\Program Files\GNU\GnuPG>
```

Para instalar la aplicación, simplemente tenemos que ejecutar el archivo "TrueCrypt Setup.exe" y aparecerá el instalador. En este escueto menú podremos personalizar algunas opciones, como la ruta de instalación, la asociación de ficheros con extensión ".tc" a la aplicación, la creación de un punto de restauración en el sistema, o la creación de accesos directos.

Una vez instalada la aplicación, podremos usar el icono situado en la bandeja de sistema para abrir la ventana principal de TrueCrypt. Mediante esta interfaz interactuaremos con la aplicación como veremos más adelante.

Compilando TrueCrypt en Linux

Lo primero, obviamente, es descargar el paquete con el código fuente del programa. Para ello, en el desplegable que hay bajo el título de Linux, en la sección de descarga de la página, seleccionaremos la opción "Other (source code)" y pulsaremos en "Download". También descargaremos la firma PGP correspondiente, y comprobaremos su validez:

```
   master@blingdenstone:~$
gpg --verify truecrypt-4.3a-
source-code.tar.gz.sig
   gpg: Signature made jue 03
may 2007 22:01:46 CEST using
DSA key ID F0D6B1E0
   gpg: Good signature from
"TrueCrypt Foundation <info@
truecrypt-foundation.org>"
   gpg:                  aka
"TrueCrypt Foundation
<contact@truecrypt.org>"
   master@blingdenstone:~$
```

Antes de compilar la aplicación, es importante tener en cuenta que es necesario tener compiladas ciertas opciones del núcleo Linux para que TrueCrypt pueda funcionar. Las opciones, y su ruta en la configuración (para Linux 2.6.23) son:

- Device Drivers ---> [*] Multiple devices driver support (RAID and LVM) --->
- [*] Multiple devices driver support (RAID and LVM) ---> <*> Device mapper support
- [*] Multiple devices driver support (RAID and LVM) ---> <*> Crypt target support
- Cryptographic API --->
- Cryptographic API ---> <*> AES cipher algorithms (i586)
- Cryptographic API ---> <*> DES and Triple DES EDE cipher algorithms
- Cryptographic API ---> <*> Blowfish cipher algorithm
- Cryptographic API ---> <*> Twofish cipher algorithms (i586)
- Cryptographic API ---> <*> Serpent cipher algorithm
- Device Drivers ---> [*] Block devices --->
- [*] Block devices ---> <*> Loopback device support

No es necesario compilar todos ellos como características del núcleo, y de hecho es más útil que sean módulos que se carguen sólo cuando sean necesarios. Si usáis una distribución de amplia difusión, como Ubuntu o Fedora, los módulos posiblemente estén ya precompilados para ser utilizados con el núcleo que incorpora; y si, como yo, sois de los que os compiláis los núcleos a mano, no tendréis ningún problema en añadir las opciones que no tengáis actualmente activadas.

A continuación, descomprimimos el paquete tar.gz y accedemos a su directorio Linux. Será necesario ejecutar el script "build.sh" con privilegios de superusuario para que funcione.

```
   master@blingdenstone:~$
tar xfz truecrypt-4.3a-source-
code.tar.gz
   master@blingdenstone:~$ cd
truecrypt-4.3a-source-code/
Linux
   master@blingdenstone:~/
truecrypt-4.3a-source-code/
Linux$ su
   Contraseña:
   blingdenstone:/home/master/
truecrypt-4.3a-source-code/
Linux#
```

Un detalle más, esta vez dedicado exclusivamente a los que compilen sus núcleos y estén utilizando la última versión estable en el momento de escribir estas líneas (2.6.23), y es que hay que hacer un poquito de bricolaje con el código fuente de TrueCrypt, que nadie se me asuste. La línea 659 del fichero "Linux/Kernel/Dm-target.c", cuyo contenido es:

```
   bio_ctx_cache = kmem_cache_
create ("truecrypt-bioctx",
sizeof (struct bio_ctx), 0, 0,
NULL, NULL);
```

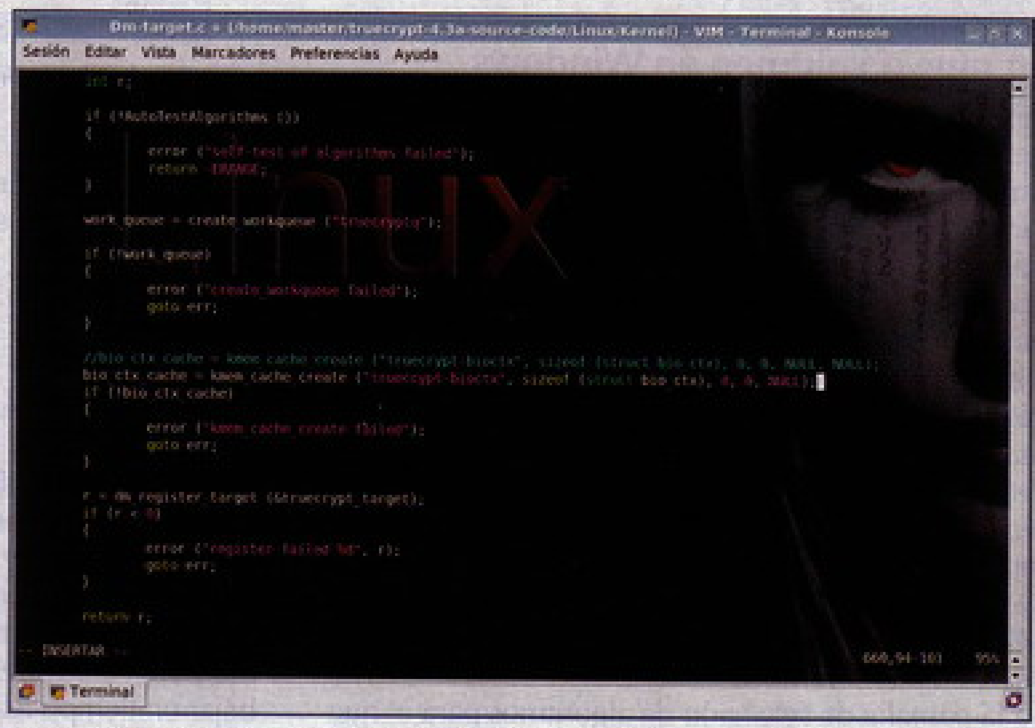
Debe ser reemplazada por la siguiente:

```
   bio_ctx_cache = kmem_cache_
create ("truecrypt-bioctx",
sizeof (struct bio_ctx), 0, 0,
NULL);
```

A partir de aquí podemos continuar todos igual, y ejecutar el script de generación, seguido del de instalación.



Comprobación de la validez de la firma en Linux.



Cambio necesario en el código para núcleos 2.6.23.

```
    blingdenstone:/home/master/truecrypt-4.3a-
source-code/Linux# ./build.sh
    Checking build requirements...
    Building kernel module... Done.
    Building truecrypt... Done.
    blingdenstone:/home/master/truecrypt-4.3a-
source-code/Linux# ./install.sh
    Checking installation requirements...
    Testing truecrypt... Done.

    Install binaries to [/usr/bin]:
    Install man page to [/usr/share/man]:
    Install user guide and kernel module to [/
usr/share/truecrypt]:
    Installing kernel module... Done.
    Installing truecrypt to /usr/bin... Done.
    Installing man page to /usr/share/man/man1...
Done.
    Installing user guide to /usr/share/
truecrypt/doc... Done.
    Installing backup kernel module to /usr/
share/truecrypt/kernel... Done.
    blingdenstone:/home/master/truecrypt-4.3a-
source-code/Linux#
```

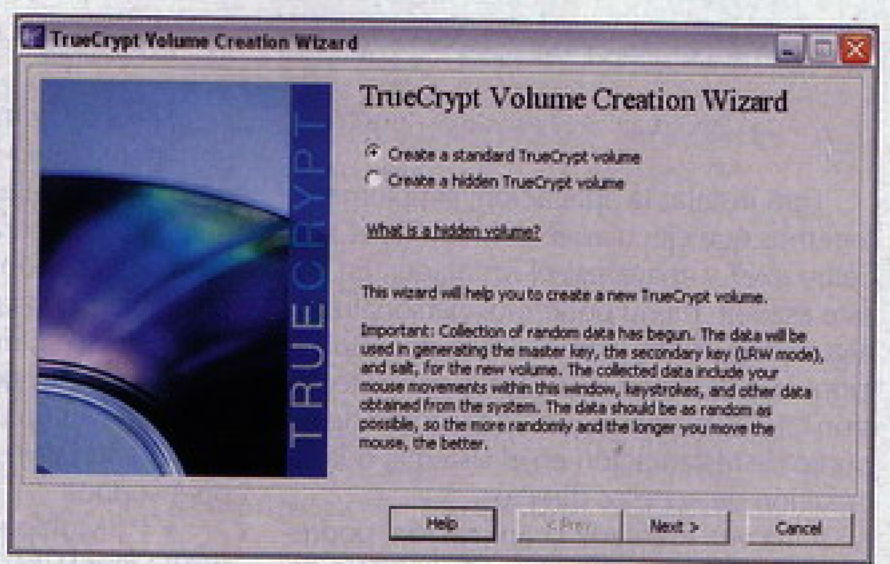
Ya tenemos disponible TrueCrypt en nuestro Linux. :-)

```
    master@blingdenstone:~$ truecrypt --version
    truecrypt 4.3a

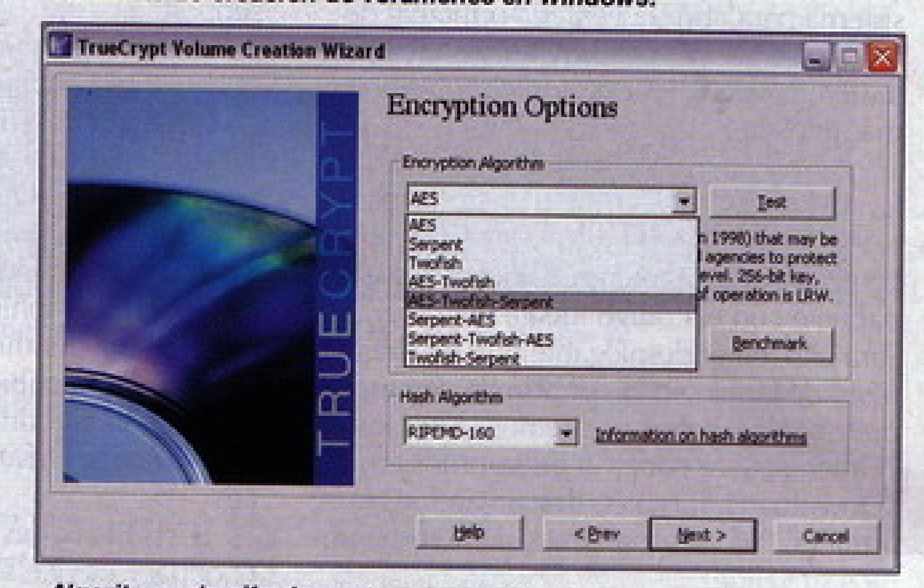
    Copyright (C) 2003-2007 TrueCrypt Foundation.
All Rights Reserved.
    Copyright (C) 1998-2000 Paul Le Roux. All
Rights Reserved.
    Copyright (C) 1999-2006 Dr. Brian Gladman.
All Rights Reserved.
    Copyright (C) 1995-1997 Eric Young. All
Rights Reserved.
    Copyright (C) 2001 Markus Friedl. All Rights
Reserved.

    Released under the TrueCrypt Collective
License 1.2

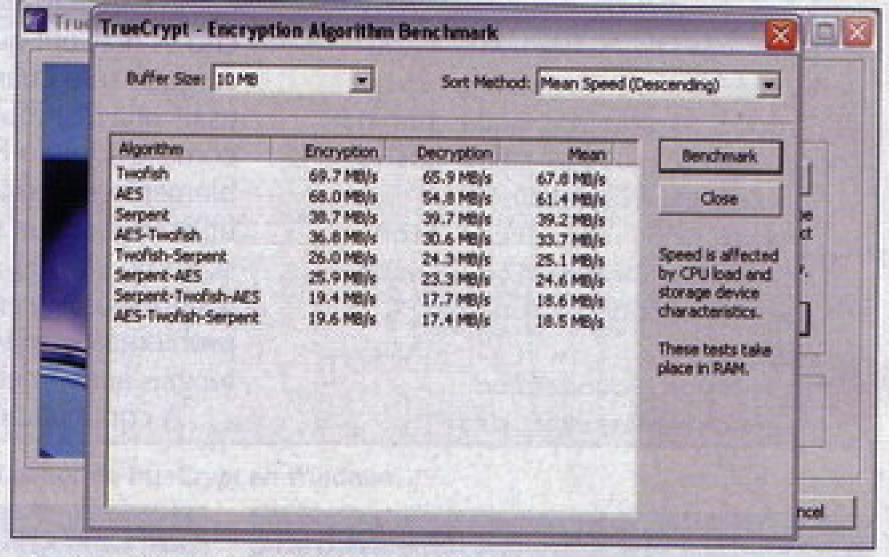
    master@blingdenstone:~$
```



Asistente de creación de volúmenes en Windows.



Algoritmos de cifrado para un nuevo volumen.



Prueba de rendimiento de los algoritmos.

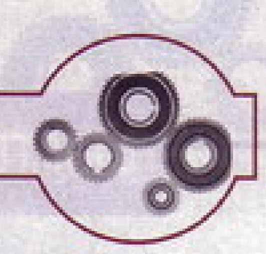
Creando un nuevo volumen en Windows

Desde la ventana principal de la aplicación, pulsando en el botón "Create volume" accederemos al asistente de creación de volúmenes. Para empezar, vamos a crear un volumen estándar, para lo que seleccionaremos la opción pertinente (viene seleccionada por defecto) y pulsaremos en "Siguiente". En la pantalla de selección de localización podremos indicar en qué fichero o partición queremos generar el volumen. Mi recomendación, por cuestiones de compatibilidad, es utilizar, siempre que sea posible y adecuado, ficheros en lugar de particiones completas; pudiendo generar un único fichero del mismo tamaño que la partición si lo que se desea es utilizar la unidad completa para almacenar datos cifrados (por ejemplo, una memoria USB). También recomiendo utilizar ficheros sin extensión, o con una extensión no obvia que no corresponda nunca con la que TrueCrypt tiene asociada (".tc"), dado que de nada sirve la "plausible deniability" aplicada al contenido del fichero si luego indicamos en su nombre qué es, en plan "contraseñas.tc"... :-P

Llegamos a la pantalla de selección de algoritmos para el nuevo volumen, donde debemos seleccionar el o los algoritmos de cifrado, así como el algoritmo de hash, que serán utilizados en el volumen a crear. Entre los algoritmos de cifrado encontramos las siguientes opciones:

- AES
- Serpent
- Twofish
- AES-Twofish
- AES-Twofish-Serpent
- Serpent-AES
- Serpent-Twofish-AES
- Twofish-Serpent

Obviamente, y según el algoritmo elegido, la velocidad de cifrado y descifrado variará ligeramente. Con los procesadores existentes en la actualidad, ninguna de las combinaciones ofrecidas por el software supondrá un problema grave a la hora de trabajar en tiempo real (máxime tratándose de algoritmos de cifrado simétricos); pero si alguien tiene una máquina no muy potente, o quiere que la carga de CPU sea mínima al escribir en el disco (por



ejemplo, porque se use muy habitualmente como soporte de almacenamiento persistente, o en un servidor), puede consultar el benchmark que el propio programa implementa para saber el rendimiento de cada una de las opciones.

En lo concerniente a los algoritmos de hash, podremos elegir entre RIPEMD-160, SHA-1 y Whirlpool. Si bien SHA-1 ha sido durante mucho tiempo el estándar de facto en cuanto a algoritmos de resumen unidireccional, hoy en día la tendencia es la de abandonar su uso en detrimento de otros algoritmos más avanzados o potentes; más aún tras la publicación de los famosos informes de colisiones de los investigadores chinos, que demostraron la posibilidad de reducir la complejidad de un ataque del cumpleaños contra el citado algoritmo.

En cuanto a RIPEMD-160, nunca ha tenido demasiada difusión al coexistir en el marco temporal de SHA-1, y además ha sido menos analizado y atacado, por lo que su seguridad es bastante más incierta que la de éste, lo cual no significa necesariamente que sea mejor. Mi recomendación personal es utilizar hoy en día Whirlpool, un algoritmo de hash especialmente pensado para máquinas de 64 bits que genera un resumen de 512 bits, lo cual es manifiestamente más seguro que las otras dos alternativas.

Tras decidir los algoritmos a utilizar, hay que indicar el tamaño del archivo (en caso de usar dicha opción) que utilizaremos. A continuación, debemos definir la contraseña que protegerá la información contenida, que obviamente deberá cumplir las clásicas máximas: no ser obvia, usar distintos juegos de caracteres, que sea larga, etcétera. Adicionalmente, podremos indicar la utilización de ficheros claves al sistema, activando la casilla de verificación pertinente y añadiendo los archivos a utilizar. La opción de generar un fichero aleatorio de clave no la recomiendo, pues la pérdida de ese archivo hará absolutamente imposible recuperar la información contenida en el volumen. Por último, sólo queda definir el sistema de ficheros (y sus parámetros) que utilizará el volumen y proceder a su formateo. ¡El nuevo volumen está listo!

Creando un nuevo volumen en Linux

Si bien existen varios entornos disponibles para utilizar TrueCrypt de manera gráfica en Linux, prefiero ver su utilización en la línea de comandos de toda la vida. Así, aprendemos a utilizarlo de forma gráfica en Windows, pudiendo hacerlo de forma muy similar en Linux, y aprendemos a usarlo mediante comandos en Linux, siendo su uso prácticamente idéntico en Windows (que también puede ser utilizado mediante consola).

Los pasos para crear un nuevo volumen en Linux son los mismos que en Windows, pero indicando las opciones de forma textual. Por ejemplo, para crear un nuevo volumen de 50Mb en "/home/master/prueba", con cifrado AES-Twofish y resúmenes hash Whirlpool, seguiremos los siguientes pasos:

```
    blingdenstone:/home/master#
truecrypt -c prueba
    Volume type:
     1) Normal
     2) Hidden
    Select [1]: 1

    Filesystem:
     1) FAT
     2) None
    Select [1]: 1

    Enter volume size (bytes -
size/sizeK/sizeM/sizeG): 50M

    Hash algorithm:
     1) RIPEMD-160
     2) SHA-1
     3) Whirlpool
    Select [1]: 3

    Encryption algorithm:
     1) AES
     2) Blowfish
     3) CAST5
     4) Serpent
     5) Triple DES
     6) Twofish
     7) AES-Twofish
     8) AES-Twofish-Serpent
     9) Serpent-AES
    10) Serpent-Twofish-AES
    11) Twofish-Serpent
    Select [1]: 7

    Enter password for new
volume 'prueba':
    Re-enter password:

    Enter keyfile path [none]:

    TrueCrypt will now collect
random data.

    Is your mouse connected
directly to computer where
TrueCrypt is running? [Y/n]: y

    Please move the mouse
randomly until the required
amount of data is captured...
    Mouse data captured: 100%

    Done: 50.00 MB   Speed:
7.01 MB/s   Left: 0:00:00
    Volume created.
    blingdenstone:/home/master#
```

La creación de volúmenes ocultos es virtualmente idéntica a los normales, tanto para Windows como para Linux, simplemente se solicitarán datos diferentes para cada uno de los volúmenes, por lo que no voy a redundar en información que ya conocemos.

Montando y desmontando volúmenes

El proceso de montado y desmontado de volúmenes ya creados es muy sencillo, y una vez realizado, dicho volumen se encontrará integrado perfectamente en el sistema de ficheros, pudiendo ser utilizado exactamente igual que si se tratara de, por ejemplo, una memoria USB.

En Windows, desde la ventana principal de la aplicación seleccionaremos la unidad en que deseamos montar el volumen y elegiremos el fichero a montar pulsando en el botón "Select File" (o "Select Device" en caso de haber utilizado una partición completa). Tras haberlo seleccionado, pulsando en el botón "Mount" podremos manejar el dispositivo virtual. Para desmontarlo, simplemente pulsaremos en el botón pertinente.

Para el sistema Linux, y desde línea de comandos, simplemente debemos invocar el programa pasándole como parámetros el fichero que contiene el volumen a montar y el punto de montaje. Con un núcleo de la rama 2.6, y la opción de cargado automático de módulos habilitada, el propio núcleo se encargará de montar el módulo de TrueCrypt así como otros módulos necesarios de forma automática. Una vez ejecutado el comando, y habiendo proveído la contraseña correcta, el volumen se integrará también en el sistema de ficheros de forma transparente.

```
    blingdenstone:/home/
master# truecrypt prueba /mnt/
truecrypt/
    Enter password for '/home/
master/prueba':
    blingdenstone:/home/
master# df
    S.ficheros          Bloques
de 1K   Usado    Dispon Uso%
Montado en
    /dev/hda3
14081400  11141584   2367584
83% /
    tmpfs
509456          0    509456
0% /lib/init/rw
    udev
10240         112     10128   2%
/dev
    tmpfs
509456          4    509452
1% /dev/shm
    /dev/hda1
24222160  14104544  10117616
59% /windows
```

```
    /dev/sda1
250308      249856        452
100% /mnt/usb
    /dev/mapper/truecrypt0

50982        0      50982    0%
/mnt/truecrypt
    blingdenstone:/home/master#

    Para desmontarlo,
simplemente utilizaremos el
parámetro "-d" del programa:

    blingdenstone:/home/master#
truecrypt -d prueba
```

Otras consideraciones

Como habréis podido comprobar, el manejo de TrueCrypt es tremendamente sencillo e intuitivo, lo cual resulta sorprendente para un software de su potencia. No obstante, siempre existen ciertas opciones avanzadas, consideraciones especiales y demás, que permiten sacarle un poco más de jugo a un programa.

En sistemas Windows, accediendo desde la pantalla principal al menú de opciones (Settings -> Preferences), podremos configurar ciertos parámetros bastante interesantes para afinar el comportamiento del programa: desmontaje automático de volúmenes cuando llevan un cierto tiempo sin usarse o se activa el salvapantallas, comportamiento del explorador de ficheros respecto al montaje y desmontaje de nuevos volúmenes, el proceso en segundo plano del programa, la conservación en memoria de las contraseñas (absolutamente desaconsejada), etc.

En Linux, ejecutando el programa sin pasarle ningún parámetro, obtendremos una lista de opciones que podemos utilizar para realizar ciertas acciones con el programa, como la creación de ficheros de clave, el uso del modo interactivo, restauración de cabeceras, etc.

```
    blingdenstone:/home/master#
truecrypt
    Usage: truecrypt [OPTIONS]
VOLUME_PATH [MOUNT_DIRECTORY]
        or: truecrypt [OPTIONS]
-i
        or: truecrypt [OPTIONS]
-c | --create | -C | --change
VOLUME_PATH]
        or: truecrypt [OPTIONS]
-d | --dismount | -l | --list
MAPPED_VOLUME]
        or: truecrypt [OPTIONS]
--backup-headers | --restore-
header FILE [VOLUME]
        or: truecrypt [OPTIONS]
--properties [VOLUME_PATH]
        or: truecrypt [OPTIONS]
--keyfile-create FILE
        or: truecrypt -h
| --help | --test | -V |
--version

    Commands:
     VOLUME_PATH
Map volume
     VOLUME_PATH MOUNT_
DIRECTORY          Map and
mount volume
         --backup-headers FILE
 VOLUME]  Backup headers of
VOLUME to FILE
     -c, --create [VOLUME_PATH]
Create a new volume
     -C, --change [VOLUME_PATH]
Change password/keyfile(s)
     -d, --dismount [MAPPED_
VOLUME]       Dismount and
unmap volume
     -h, --help
Display detailed help
         --keyfile-create FILE
Create a new keyfile
     -i, --interactive
Map and mount volume
interactively
     -l, --list [MAPPED_VOLUME]
List mapped volumes
         --properties [VOLUME_
PATH]       Display properties
of volume
         --restore-header FILE
 VOLUME]  Restore header of
VOLUME from FILE
         --test
Test algorithms
     -V, --version
Display program version and
legal notices

    Options:
         --cluster SIZE
Cluster size
         --display-keys
Display encryption keys
         --display-password
Display password while typing
         --disable-progress
Disable progress display
         --encryption EA
Encryption algorithm
         --filesystem TYPE
Filesystem type
         --hash HASH
Hash algorithm
     -k, --keyfile FILE|DIR
Keyfile for volume
         --keyfile-add FILE|DIR
New keyfile for volume
     -K, --keyfile-protected
FILE|DIR    Keyfile for
protected volume
     -M, --mount-options
OPTIONS          Mount options
     -N, --device-number NUMBER
Map volume as device number
         --overwrite
Overwrite files without
confirmation
     -p, --password PASSWORD
Password for volume
         --password-tries
NUMBER         Password entry
tries
     -P, --protect-hidden
Protect hidden volume
         --random-source FILE
Random number generator input
file
         --quick
Use quick format
         --update-time
Do not preserve timestamps
     -r, --read-only
Map/Mount volume as read-only
         --size SIZE
Volume size
         --type TYPE
Volume type
     -u, --user-mount
Set default user and group ID
on mount
     -v, --verbose
Verbose output

     MAPPED_VOLUME = DEVICE_
NUMBER | DEVICE_NAME | MOUNT_
POINT | VOLUME_PATH
    For a detailed help, use
--help or see truecrypt(1) man
page.
    For more information,
visit <http://www.truecrypt.
org/docs/>.
    blingdenstone:/home/master#
```

Concluyendo

En un mundo donde el derecho a la intimidad y a la privacidad está tan alarmantemente amenazado, donde ladrones, spammers, entidades de gestión y el propio gobierno se dedican a espiarnos sin contemplaciones; cada pequeño rincón de seguridad al que podamos aferrarnos es un auténtico tesoro.

TrueCrypt, definido -de forma totalmente acertada- por la gente de Kriptópolis como "la mejor herramienta de cifrado disponible en la actualidad", es (junto a GnuPG y alguno más) uno de esos programas criptográficos que resultan absolutamente imprescindibles en los tiempos que corren.

Como dijo Benjamin Franklin, "tres podrían guardar un secreto si dos de ellos hubieran muerto". Guardad vuestros secretos a buen recaudo.

Feliz cifrado. :-)

Ramiro C.G. (alias Death Master)
death_master@hpn-sec.net
http://www.death-master.tk/


alg@rroba
123
AÑO 9 (??? ¿TODAVÍA?), NÚMERO 123
especial friki gadget
CELEBRANDO EL DERROCHE, OIGA

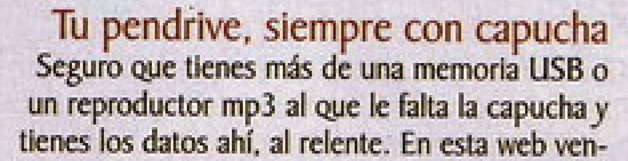


¿Cómo? ¿Que no esperábais algo así? Pero bueno, que vienen las Navidades y las rebajas de enero, ¿qué otra cosa se puede hacer? ¡Pues comprar, solo eso!



World of Warcarft te deja limpito

Y no nos referimos a que te saque los cuartos. Si eres fan del juego de Blizzard, es el momento de lavarse las manos con este exclusivo jabón. Que es para usarlo, no es un adorno.
http://www.etsy.com/view_listing.php?listing_id=7483677



Tu pendrive, siempre con capucha

Seguro que tienes más de una memoria USB o un reproductor mp3 al que le falta la capucha y tienes los datos ahí, al relente. En esta web venden capuchas para tu memoria, y así protegerla de suciedad, polvo y golpes.
http://www.rookaps.com/







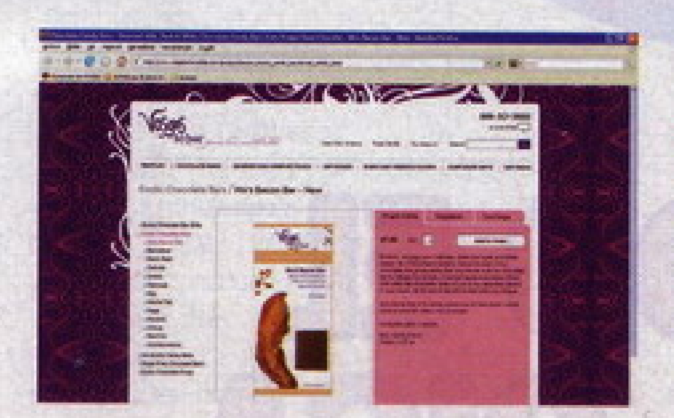
Para el guitarrista que llevas dentro

Conéctala a la tele y a tocar clásicos del rock al más puro estilo Guitar Hero, pero sin consola de por medio. Incluye 10 canciones estupendas, como Smoke on the Water, I Love Rock and Roll y You Give Love a Bad Name.
http://www.dreamgear.net/view-product.asp?idpr=618

¡A volar!

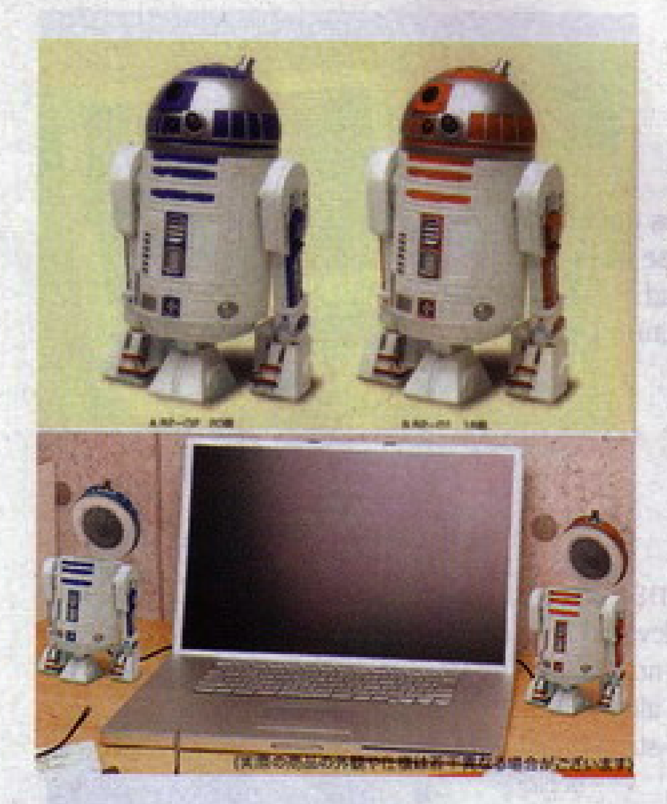
Seguimos con la moda de despertadores coñazo. Pero coñazo de verdad. Este modelo tiene una hélice en la parte superior que, cuando suena la alarma, sale disparada por el aire. La alarma no dejará de sonar hasta que no cojamos la hélice y la volvamos a colocar en el despertador. Lo dicho, coñazo.
http://www.microsiervos.com/archivo/gadgets/despertador-volador.html





Bacon de chocolate, o chocolate de bacon

Mmmmm. El producto definitivo para las arterias y las cartucheras. Una fina (?) mezcla de bacon y chocolate, que nos trae dos de los sabores más queridos por todo friki, unidos en una combinación... Letal.
http://www.vosgeschocolate.com/product/bacon_exotic_candy_bar/exotic_candy_bars



El Sonido de las Galaxias

Hala, el producto Star Wars del mes, que no falte. Hoy toca altavoces con forma de unidades R2. Por fin podremos quitar los altavoces blanquitos esos de tienda de informática tan genéricos e impersonales.
http://technabob.com/blog/2007/10/17/r2-d2-speakers-play-more-than-beeps-and-blips/



¡Venganza!

Véngate de tus vecinos con los sonidos más pesados del universo. Una sesión de sexo apasionado, el sonido de unos tacones altos recorriendo el pasillo y martilleando el oído, un taladro agujereando la pared... Un montón de pistas para molestar y vengarnos de los vecinos. Incluye tapones para nuestros oídos, faltaría más.
http://wishingfish.com/revengecd.html



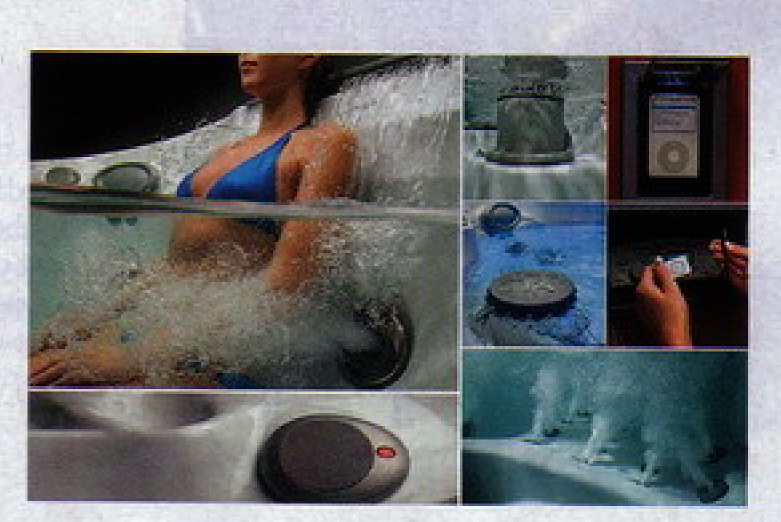
Green Power!

Nada como las Fuerzas de la Naturaleza para alimentar y recargar las baterías de tu mp3 o iPod, porque no siempre se tienen enchufes a mano. Los gadgets también tienen su parte ecológica.
http://www.hymini.com/



Al rico cenicero sexista

¿Quién querría apagar sus cigarros en un cenicero con la forma de una mujer desnuda haciendo una felación? Pues debe haber gente disponible, o si no, no sacarían estas aberraciones. En fin.
http://www.tokyomango.com/tokyo_mango/2007/10/naked-girls-mou.html



iPod + Jacuzzi

Encima cachondeo. Los pisos cada vez más caros y más pequeños, y van y sacan los jacuzzi tamaño enorme con conexión para el iPod y relajarse aún más, entre las burbujitas y la música.
http://gizmodo.com/gadgets/home-entertainment/new-jacuzzi-j400-hot-tub-is-all-about-the-ipod-312110.php



especial FRIKI GADGET

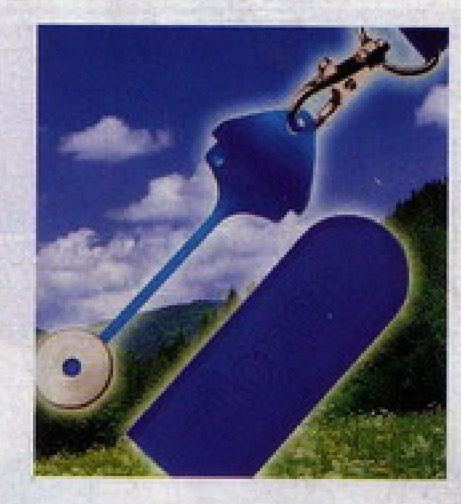


Ratón Minnie

No, no es que sea un ratón tamaño mini, es que es un ratón de Minnie, la eterna novia de Mickey. O sea, que no se han casado. ¿O sí? A tal nivel de frikismo no llegamos, la verdad.
http://geekstuff4u.com/product_info.php?manufacturers_id=&products_id=626



Zilopop, para el mal aliento



Si el mal aliento te acompaña todos los días, lleva encima el Zilopop, un artilugio con forma de llavero que nos metemos en la boca unos segundos y hala, mal aliento fuera.
http://www.random-good-stuff.com/2007/10/16/stainless-steel-vs-bad-breath/



Altavoces enlatados

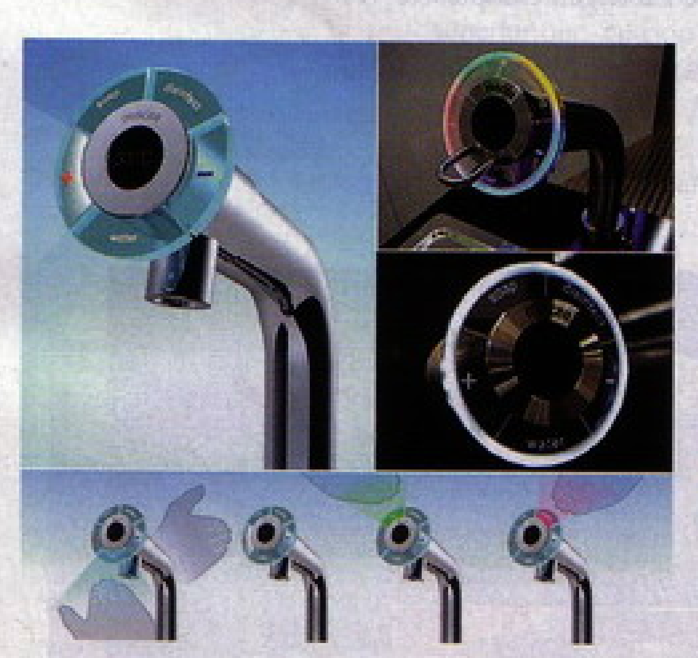
Si el espacio es un problema, podemos hacernos con estos dos pequeños altavoces, que vienen en forma de lata. Los desenroscamos para usarlos, y cuando no los necesitemos, los volvemos a poner en forma de lata y ganamos unos centímetros cúbicos.
http://www.everythingusb.com/coagent_music_can_usb_speakers_13521.html



Mininevera USB



Esta mininevera tiene capacidad para una sola lata o vaso, pero tiene dos usos. Enfría nuestra bebida, o la calienta. Un buen invento que tampoco ocupa mucho espacio. Eso sí, ya mismo nos hace falta un puerto de 500 USB.
http://www.usbgeek.com/prod_detail.php?prod_id=0711



El grifo mágico

Atrás quedaron los grifos tradicionales, que solo echan agua o, como mucho, jabón. Este grifo multiusos dispensa hasta sopa o desinfectante. ¿Se podrá configurar para el calimocho?
http://gizmodo.com/gadgets/gadgets/miscea-touchless-faucet-magically-spews-out-water-soap-who-knows-what-else-310451.php





Tachikoma de andar por casa

Los fabulosos robots Tachikoma de la saga Ghost in the Shell ahora pueden acabar en tu escritorio. Este modelo puede leer tu correo, moverse, arrancar aplicaciones de tu ordenador y mucho más.
http://www.akihabaranews.com/en/news-14945-Get+your+own+Tachikoma+robot+from+Bandai.html



Reloj estilo Frankenstein

Luces terroríficas para un despertador rarito pero resultón. Y dale con los despertadores, no nos extraña que nos odiéis.
http://www.newlaunches.com/archives/the_lightning_alarm_clock.php





El donut-matic

Menudo regalo. Máquina portátil para hacer rosquillas en casa. No se incluye desfibrilador para cuando el corazón no dé más de sí por la grasa.
http://www.random-good-stuff.com/2007/10/14/present-for-a-cop/



Loro guapo, guapo

Nos vamos de nuevo a los 80 con un espléndido dock que tiene la forma de un boombox (o loro, en plan castizo) para poner nuestro iPod y llevarlo a la playa con Los Chichos a toda leche.
http://www.suck.uk.com/product.php?rangeID=75





Perrito hidratado, perrito feliz

Este bol para el agua del perro tiene un dispensador con forma de taza del WC. Para que el perro de casa satisfaga su ilusión de beber del retrete de verdad.
http://www.bookofjoe.com/2007/10/worlds-most-t-1.html



especial FRIKI GADGET

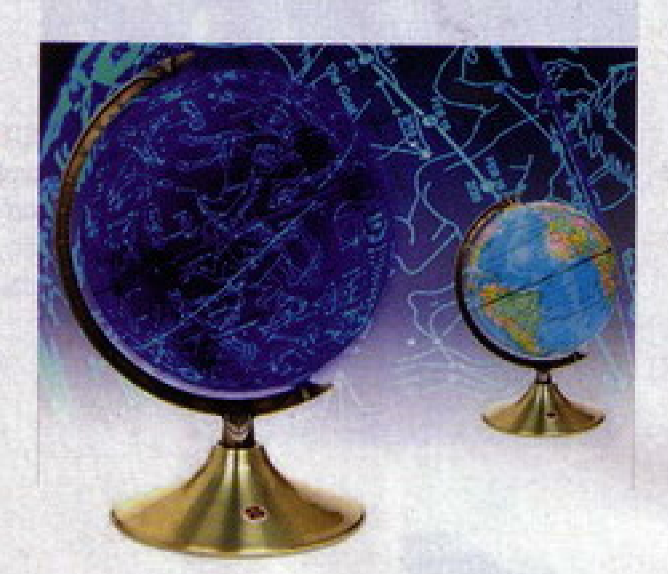


Pinball para el sótano

Estupendo pinball digital para poner en el estudio o sótano de casa y alucinar un rato dándole al flipper. Nada menos que 12 mesas distintas en una sola, como si tuviéramos una versión deluxe de un videojuego de pinball. Mola.

http://extremetoysforboys.com/index.php3/item/item/UltraPin%20-%20Digital%20Pinball%20Machine.html





Las luces de la noche

El típico globo terráqueo para estudiar ha quedado atrás. Llega el globo con sensores de luz, que reproducen unas luces de lo más chic cuando haya oscuridad en la habitación.

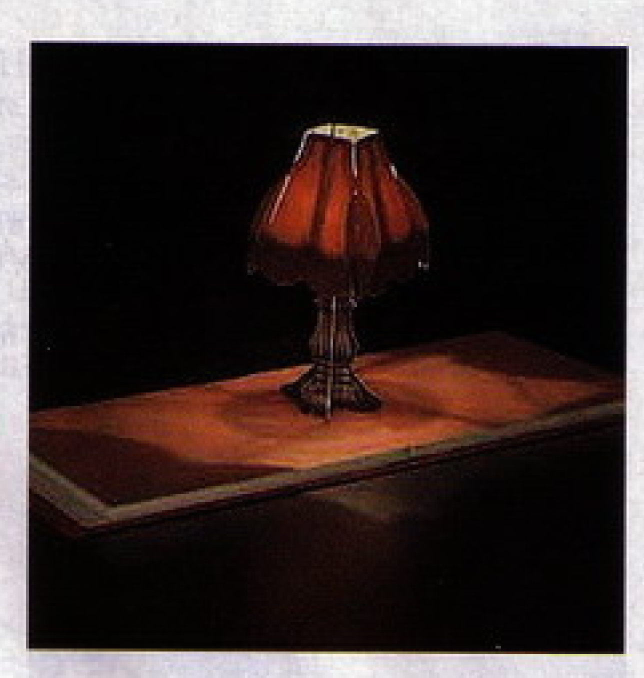
http://www.geekalerts.com/glowing-globe-earth-transforms-to-sky-at-night/



Pesca con la Wii

En plena vorágine de manditos para acoplar al mando de Wii, nos llega la caña de pesca... ¡Y el pececito de plástico para que todo sea más real! La NetxGen ha llegado.

http://www.maxconsole.net/?mode=news&newsid=22471



La lámpara-libro

Otro artículo más para los faltos de espacio: un libro que, al abrirlo, despliega una bonita lámpara para la mesita de noche. La decoración hortera no ocupa lugar, y nunca es suficiente.

http://www.uncrate.com/men/home/lighting/book-of-lights/

El ordenador Transformers

Los niños también se merecen tener su ordenador. Pasados están los días del SuperQuique o como se llame, ahora lo que mola es el ordenador Transformers, con sus programitas y sus minijuegos. No lleva Ubuntu, ojo.

http://www.geekalerts.com/transformers-learning-laptop/



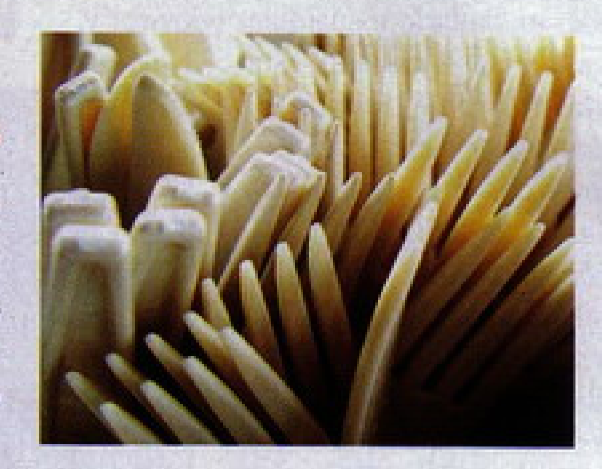


Cuchara para el bebé

Una ingeniosa cuchara que dosifica la comida que le vamos dando al pequeñajo o pequeñaja de casa. En su interior metemos la comida y la vamos pasando directamente a la cuchara, tan solo pulsando.
http://www.gadgetgrid.com/2007/11/05/squirt-baby-food-dispensing-spoon/



A comer patatas con patatas



He aquí los cubiertos comestibles. O sea, cucharas, tenedores y cuchillos hechos de patata. Para luego no dejar, literalmente, nada en el plato. Yum.
http://gizmodo.com/gadgets/dining/spudware-cutlery-eat-potatoes-with-potatoes-310558.php



¡Pato-control!

Después de tanto patito de juguete que en realidad es algo con fines sexuales, como estamos viendo últimamente, era hora de recuperar el sencillo e inocente pato. O sea, un pato de juguete corriente y moliente. Bueno, éste en concreto tiene control remoto, que siempre viene bien alguna novedad.
http://www.play.com/Gadgets/Gadgets/-/434/534/-/3469714/Remote-Control-Rubber-Duck/Product.html?searchtype=genre#



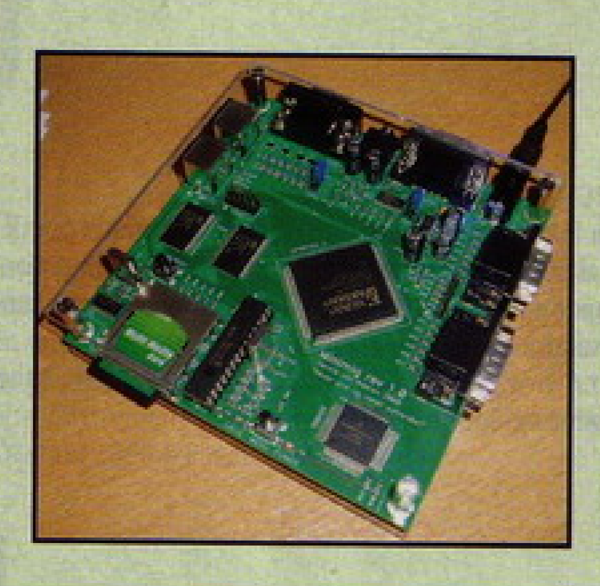
El sujetador-bandeja

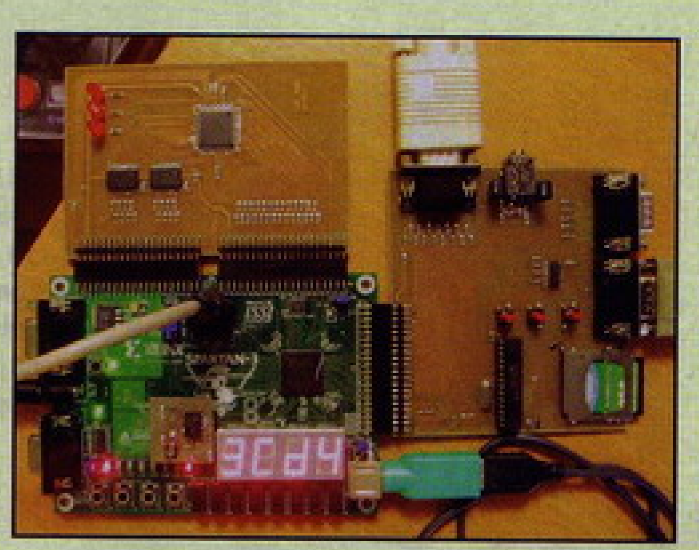
Invento rarísimo de, no podía ser de otra forma, los japoneses. Un sujetador con sitio para la comida del día. Una copa para el arroz cocido y la otra para el tazón de sopa y/o tallarines. Qué cosas.
http://gizmodo.com/gadgets/appetite-lost/bra-its-whats-for-dinner-319887.php

WEB del mes

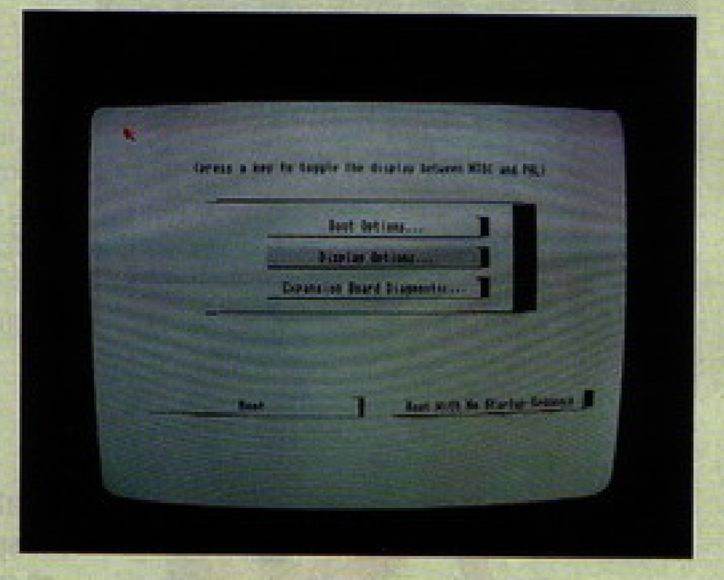
http://home.hetnet.nl/~weeren001/

Seguro que muchos conocéis esos entrañables joysticks que tienen un montón de juegos de Commodore 64, por ejemplo. Y también conoceréis el interesante One Chip MSX, todo ello gracias a la tecnología FPGA. Pues bien, en esta página vemos otro no menos atractivo proyecto, el Minimig, algo así como el One Chip Amiga, usando el citado FPGA. Y es que ¿a quién no le gustaría tener un Amiga 500 en tamaño reducido, para poder enchufarlo a cualquier televisor y jugar con las glorias de esta plataforma? Pues no pocos usuarios querríamos hacernos con un cacharro de estos, la verdad. Que una cosa es tener un montón de emuladores y otra poder llevar un pequeño aparatito a todas partes con unos cuantos juegos selectos de Amiga 500. Toda la información y los avances del proyecto Minimig en esta página.





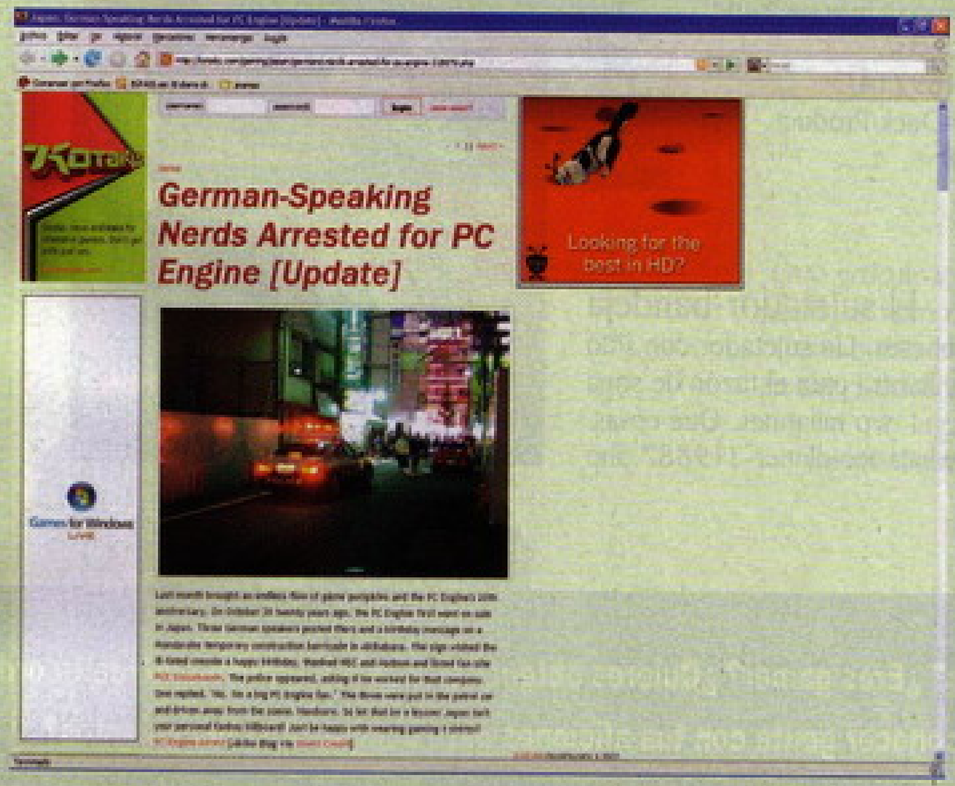






WEB Chorra

http://kotaku.com/gaming/japan/germans-nerds-arrested-for-pc-engine-318674.phpctid/17?cpncode=11-34199167-2&srccode=cii_10043468



Bueno, bueno, una cosa es ser muy fan, otra muy friki y otra un vándalo. A ver, explicamos un poco el tema. Recientemente se cumplió el vigésimo aniversario de la consola PCEngine de NEC, una gran máquina que, aunque no tuvo la resonancia de las consolas de Sega y Nintendo en la era de los 16 bits, tiene no pocos buenos títulos. Pues bien, el pasado 30 de octubre, coincidiendo con su salida a la venta hace ya 20 años, tres fans suizos quisieron celebrarlo en Akihabara, Japón. Se fueron a una obra y en las vallas de la misma colocaron fliers conmemorando el cumpleaños de la consola. En ese momento apareció la policía y arrestó a los tres suizos. Habéis leído bien. Se los llevaron al cuartelillo. Moraleja: cuidado con las formas de celebrar nuestro amor por la retroinformática, puede ser confundido por vandalismo o propaganda política. Glups.

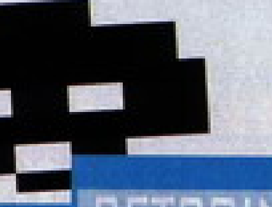


STAFF

"Hala, a comprar que luego vienen las vacas flacas": Gaby López
"Pero, ¿de dónde voy a sacar dinero para todo esto?": Carlos Verdier
"¿Y cuánto me ha sobrado del peaso de Mac que me he comprado?": Pablo Guil



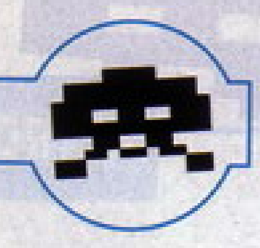
FONDOS
Envía AFONDO y su código al 7372
Ej: AFONDO 81171 o llama al 806 464 172
2313 2316 2318 2321 2323
3625 3637 3648 3654 3661
50041 5734 5735 5740 5742
5799 5817 5843 5854 5931
727 728 81861 81907 81909
82129 82207 82209 82211 82214
82233 82237 82236 82240 82241
2335 2337 2348 2350 2352
3662 50007 50012 50023 50034
5746 5749 5764 5765 5768
+18
VIDEO REAL
¡Las escenas mas divertidas y mas calientes!
Envía APELI y su código al 7372. Ej: APELI 62015 o llama al 806 464 172
64322 64303 64522
62016 62018 62025 64314 64342 64523
62013 62020 62026 63110 63106 63120
62011 62007 62034 63102 64289 64466
SONIDOS REALES
Envía SONID y su código al 7372.
Ej: SONID 9370 o llama al 806 464 172
F1 Alonso 9843
Sainz Pasada 9844
Gasol Pelota rompe cristal 9845
Pedrosa acelerando 9846
Bobo solemne 9831
España - España España oe oe oe 9793
Españoles Franco ha muerto 9665
kill bill silvido 9476
Coge el telefono que me da la risa 9746
Orgasmo placentero 9761
RELATOS
Los relatos eróticos mas apasionantes!!
TE EXCITARAS COMO NUNCA!
Envía RELAT al 7372
HENTAI
Los fondos manga y hentai mas sexy!!!
Envía HENTAI al 5099
JUEGOS
Envía AGAME y el código del que quieras al 7372
Ej: AGAME 4460
¡Los juegos mas fuertes!
4465
4460
MOVILES COMPATIBLES:
TOP
GRUPO CODIGO
Rompe 70682
A pain that I'm 70684
No Bravery 70691
Mentiras Piadosas 70692
Muñeca de trapo 70694
Bloody Mary 70695
Stupid Girls 70700
My hips dont lie 70714
Opa yo via ace un corral 70722
L.O.V.E. 70726
No quiero verla mas 70732
Pa mi guerrera 70737
Me Voy 70740
Dulce Locura 70742
One 70743
Beep 70748
Dani California 70751
Chots 70756
Corazon de fuego 70759
Ugly 70760
Pump it 70761
REGGAETON
El baile del... 70328
Asesina 70403
Mueve mami 70404
Hasta cuando 70356
Gasolina 70357
Lo que paso 70386
Eres mi baby 70555
Dale Don Dale 7584
Dile 70308
Don keo 70561
Ella y yo 70559
Luna 70387
Otra noche 70388
Pobre diabla 70389
POLIFONICOS
Envía ROLI y su código al 7372
Ej: ROLI 70543 o llama al 806 464 172
SUPERVENTAS
Push the button 70631
Gold Digger 70630
Window Shopper 70629
Pon De Replay 70627
Belly Dancer 70624
Ass like that 70623
Oh 70622
Stick With You 70621
We be burning 70619
Lets Get Down 70617
Come Clean 70615
Goodies 70611
High 70608
Fly 70603
Dare 70600
Advertising Space 70599
Jesus of suburbia 70597
Beverly Hills 70595
All About Us 70594
Dont Cha 70592
Because of You 70589
Yellow Brick Road 70588
My Humps 70583
Tripping 70579
Dont Lie 70578
Cool 70576
Fix You 70574
Wise Men 70572
Ghetto 70571
The One 70569
I dont care 70557
Madonna - Hung up 70556
Shakira - Dont bother 70553
Anastacia - Pieces of a dream 70552
Juanes - Para tu amor 70550
LATINO
El Profe 70665
Como Cambia la vida 70662
Mi mundo si ti 70660
Besos 70655
Marta, Sebas, ... 70654
Querida enemiga 70652
Vacaciones 70580
Rutinas 70551
Nada fue un error 70516
Te regalo 70514
Amar sin ser amada 70503
No 70502
Nada es para ... 70501
Damelo 70500
Ciudad perdida 70455
Ojos de cielo 70430
A la hora de amar 70410
Mi barrio 70407
La tortura 70362
La camisa negra 70361
Volverte a ver 70313
No entiendo 7963
Sentada aqui en ... 7915
Eres 7913
Obsesion 7818
Se me ocurre amarte 7567
Objection 7500
Nuestra vida 70658
Las Palabritas 70527
Te haria una casita 70518
Oleada 70468
La quinta estación - Perdición 70469
Paulina Rubio - Otro tequila 70470
Seguridad Social - A tontas y...70463
La musicalite - Brisa 70464
CINE/Tv
Matrix Reloaded 7118
La pantera rosa 7121
Sex in the city 7125
Terminator 7126
X-files 7130
Rocky 7518
El ultimo mohicano 7586
Lord Of The Rings 7600
Superman 7622
Tiburon 7624
Brave Heart 7698
Gladiator 7703
Angeles de Charlie 7866
A-Team 7867
Austin Powers 7868
Batman 7869
Conan El Barbaro 7873
Exorcista 7874
Fame 7875
Flashdance 7876
Friends 7877
Harry Potter 7879
Incredible Hulk 7880
Miami Vice 7881
Top Guns 7882
Armageddon 7900
Beverly Hills Cop 2 7903
CSI 7904
El Padrino 7906
Ghost 7908
La Roca 7909
Love Story 7910
Spiderman 70102
La Fabrica de Chocolate 70558
Kill Bill II - Silvidos 70659
ANIMACIONES
Envía XTREME y su código al 7372 Ej: XTREME 4001
4398 4393 4388 4375
4373 4372 4368 4366
4337 4335 4334 4330
4322 4325 4104 4603
Nos reservamos el derecho de utilizar los datos enviados para posibles operaciones futuras. No obstante disponen de un derecho de acceso, de rectificacion y de limitación de datos, en lo que se refiere, ya que somos los únicos destinatarios. Mas contenidos en WWW.MOVILXTREMO.COM



La capitalización de los sistemas

¿Un alegato en contra de lo gratuito?

La Ciencia puede ser divertida. Miren Beakman's World si no me creen. Emitido en televisiones autonómicas como TV3, TVG, Telemadrid, Canal 9, Canal Sur y ETB, y hasta hace poco a nivel nacional por el canal Cuatro. Divertida y desternillante. La Economía, sin embargo, suele ser aburrida; y no sé porqué, ya que se trata de lo que más nos interesa. Prepárense entonces, que me pongo la bata color pistacho, me cardo el pelo a lo loco y ¡bada bing, bada bang, bada vamos allá! ¡Vintageoscopio!



Piedra - Papel - Tijera

Les voy a escribir sobre un tema verdaderamente positivista y animoso, tomando como punto de partida un documental que se estrenó el pasado mes de septiembre en el Calgary International Film Festival, ochenta y ocho minutos con el nombre de 'Rock Paper Scissors', que traducido al cristiano sería 'Piedra Papel Tijera'. Ésto que podría entenderse producto del morapio tabernero más peleón es real, es un documental sobre el campeonato internacional del juego de 'Piedra Papel Tijera'. Que sí, campeonato internacional del juego de 'Piedra Papel Tijera', no hace falta que lo relean otra vez.

Desde hace unos añitos los hermanos Douglas y Graham Walker, canadienses, montan un tinglado asombroso alrededor de ese juego infantil. Huelgo explicarles las reglas de juego, que suficiente apuro estoy pasando escribiendo sobre algo así. Campeonato internacional. Manda huevos, señor Trillo, que lo pone en www.rpsfilm.com.

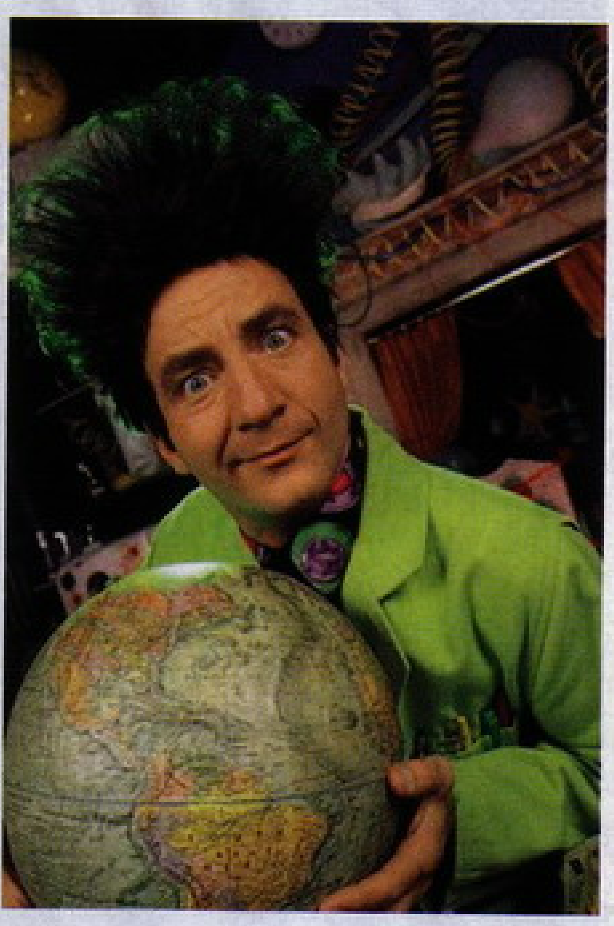


El asunto es que a Canada acuden equipos de todo el mundo -desconozco si nosotros contamos con selección nacional, que si es que no, ya saben-, equipos uniformados, entrenados y toda la pesca, y compiten y lloran cuando pierden y se emborrachan cuando ganan. Desde aquí el documental versa en algo más, en la repercusión mediática, en el mercadeo que se hace del evento. Prensa y televisión cubriendo cada combate, nenas monas enseñando ombligo y perniles haciendo publicidad de patrocinadores... ríanse ustedes del tinglado de la Vuelta Ciclista a España. Así pues, el documental utiliza el campeonato en si como excusa para dejar sobre el tapete lo que genera una competición tan infantil y nulamente trascendental como es jugar a 'Piedra Papel Tijera': dinero, carretadas de dinero.

¿Verdad que Beakman más 'Piedra Papel Tijera' ya les empieza a parecer divertido? Pues es eso, cómo la Economía en lo vintage puede ser algo digno -y diría que necesario- de tratar, y más aún cuando hablamos de producciones recientes que afectan y deberían interesar a todo usuario y simpatizante de los ordenadores domésticos y consolas de videojuegos obsoletos.

El estado de las cosas

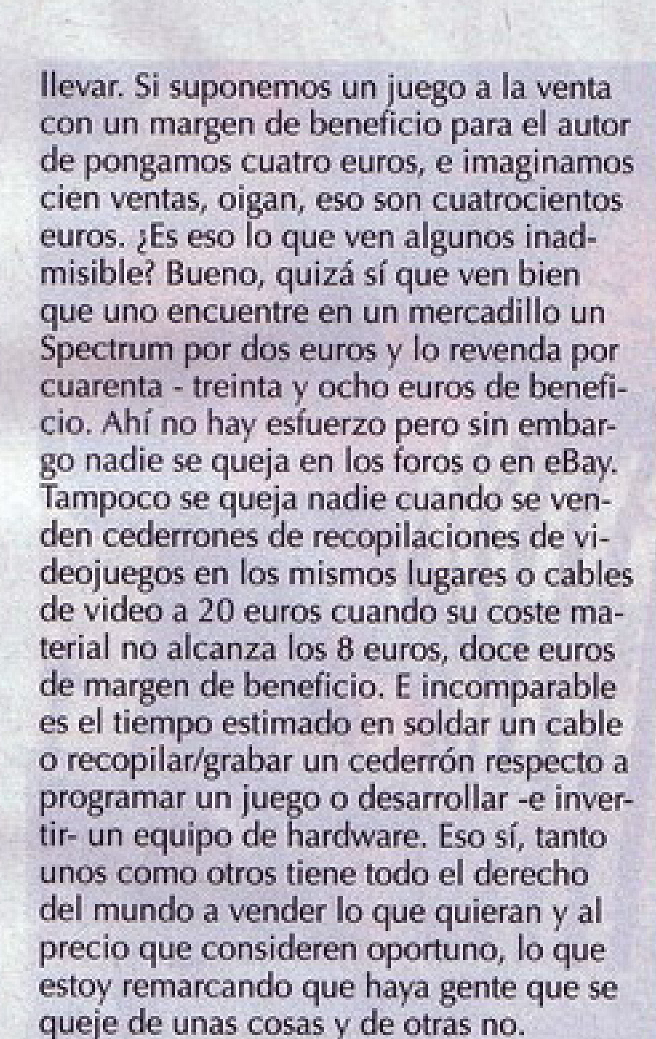
Como nota informativa, en 1990 habían en España unos 20.000 usuarios de Amiga. Seis años después, en 1996, quedaban unos 5.000 usuarios en activo según fuentes del momento, Amiga.Info mediante. Once años después ¿cuántos deben quedar contando supervivientes y reenganchados? ¿Y de Spectrum, Amstrad, Commodore o MSX, máquinas y sistemas un poco más añejos? Cientos de cada, seguramente quinientos sea una cifra que ni para tí ni para mí. Esos quinientos -o menos- usuarios de Spectrum, Commodore y Amstrad ¿no son, acaso, mercado potencial para desarrollos de carácter doméstico, para producciones hechas en casa sin necesidad de estar respaldadas por compañías de verdad? Si una bobada como el 'Piedra Papel Tijera' ha movido lo que ha movido, seguro que cualquiera de nuestras maquinitas puede mover lo mismo. O más.



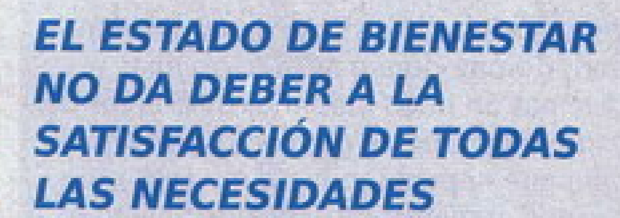
¿YA SE HAN OLVIDADO CÓMO EMPEZARON LAS PRIMERAS EUSKAL PARTY Y HASTA DONDE HAN EVOLUCIONADO?

Cuando se habla del tema siempre sale el figura que con semblante lapidario suelta aquello de 'aquí nadie se va a hacer rico vendiendo productos' o 'si alguien espera hacerse millonario ya puede ir poniéndose cómodo' como diciendo que cobrar por un producto o producción está feo. Un desarrollo de hardware, señor figura, no se genera espontáneamente, no hay unos duendecillos que por la noche salen de sus madrigueras, soldan y pagan componentes venidos de allende los mares; un desarrollo de software no se produce por escritura automática, el programador no entra en trance y teclea instrucciones que se convierten en movimiento en pantalla. Si cualquiera de ustedes cobra por ir a trabajar creo entender que cualquier trabajo debe ser remunerado, o bien permanecer el derecho a retribución.

Rico desde luego que uno no se hará programando ahora para Spectrum pero un buen pellizquito sí que se puede



llevar. Si suponemos un juego a la venta con un margen de beneficio para el autor de pongamos cuatro euros, e imaginamos cien ventas, oigan, eso son cuatrocientos euros. ¿Es eso lo que ven algunos inadmisible? Bueno, quizá sí que ven bien que uno encuentre en un mercadillo un Spectrum por dos euros y lo revenda por cuarenta - treinta y ocho euros de beneficio. Ahí no hay esfuerzo pero sin embargo nadie se queja en los foros o en eBay. Tampoco se queja nadie cuando se venden cederrones de recopilaciones de videojuegos en los mismos lugares o cables de video a 20 euros cuando su coste material no alcanza los 8 euros, doce euros de margen de beneficio. E incomparable es el tiempo estimado en soldar un cable o recopilar/grabar un cederrón respecto a programar un juego o desarrollar -e invertir- un equipo de hardware. Eso sí, tanto unos como otros tiene todo el derecho del mundo a vender lo que quieran y al precio que consideren oportuno, lo que estoy remarcando que haya gente que se queje de unas cosas y de otras no.



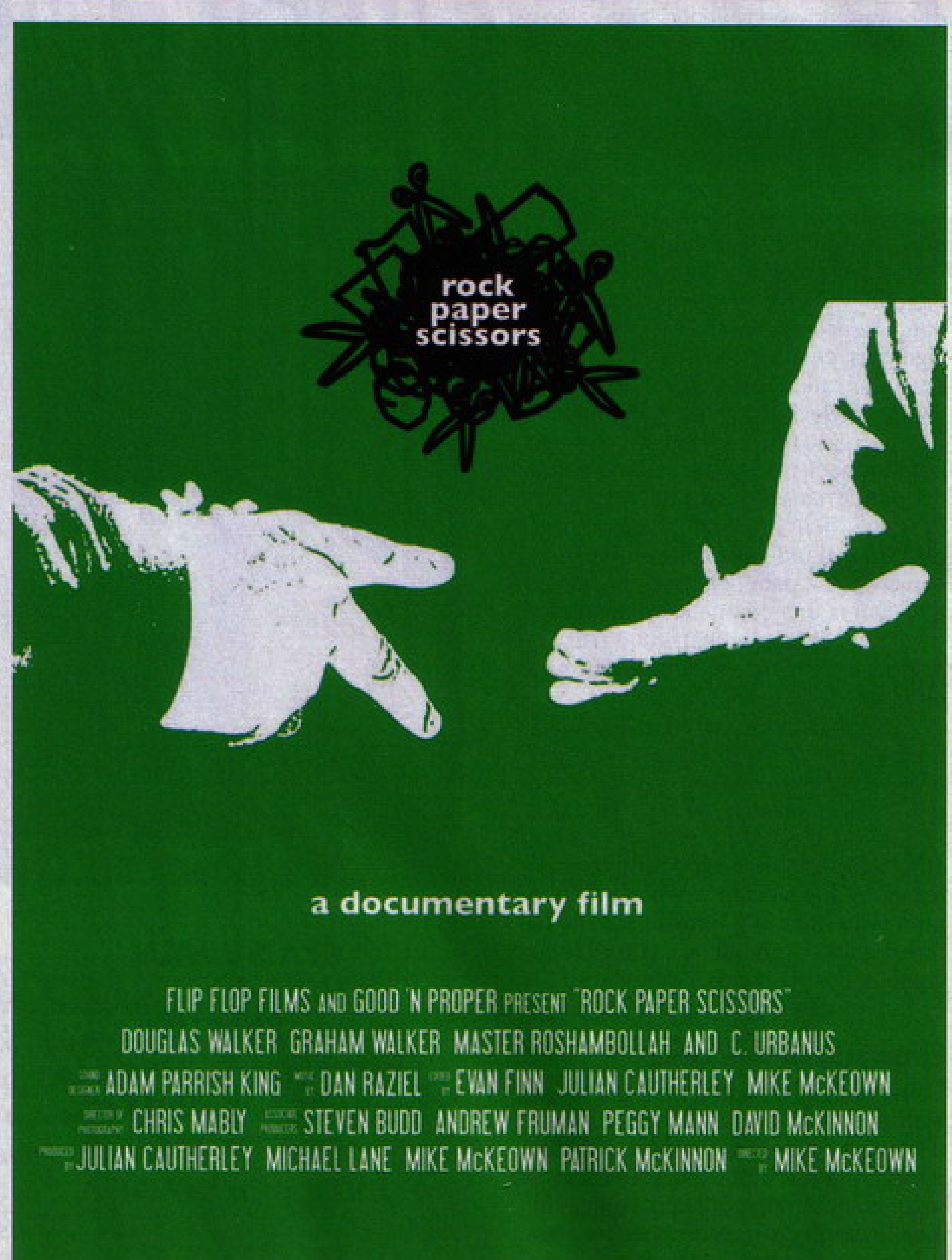
EL ESTADO DE BIENESTAR NO DA DEBER A LA SATISFACCIÓN DE TODAS LAS NECESIDADES

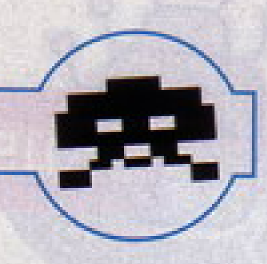
Karl Marx Headroom

Reflexionen en las ventajas de pagar por productos relacionados con lo vintage. Tendrían derecho a protestar si el producto no cumple expectativas, podrán exigir una calidad que en lo gratuito es de obligada aceptación. El autor recibiría una recompensa monetaria que ora le serviría para llenar el depósito de gasolina del coche, ora le sería servicial para llevar a su señora y a los niños al Port Aventura, Tierra Mítica o al Warner Bros Park que tocase. Una cosa y la otra le debería incentivar a, primero, generar más producciones, y segundo, que esas sean de mejor calidad. Y el efecto dominó, cuando patrocinadores, cadenas de televisión y otros entes percibieran el mogollón que se produce cuando un montón de disidentes se juntan y se convierten ante sus ojos en un mercado potencial de consumidores. Como con el campeonato internacional de 'Piedra Papel Tijera'. ¿O es que ya han olvidado cómo empezaron las primeras Euskal Party y hasta donde han evolucionado?

La idea del software libre -que no código abierto-, aquello de la aldea global, eso de la libre distribución y del derecho de pernada sobre todo lo que toca la







SGAE está muy bien para productos y sistemas actuales, cuentan con infinito número de productores y aunque caigan unos pocos por el camino siempre hay más que tomarán el relevo. En lo vintage no, estamos nosotros y nadie más. Bueno, sí, están las compañías de telefonía celular y grandes como Sega, Taito y Namco que van sacando disimulaciones de juegos pretéritos para sus consolas de juegos actuales pero no es la cosa real, que eso es otro tema.

El pensamiento anárquico ese de que todo lo informático y videojueguil debe ser gratis alegando su elevado precio es una charlotada. Bien que todos pagamos por un cafetito o por una cervecilla, bien que pagamos por unos cederrones para grabar Dios sabe qué. Y bien que el jornalero quiere cobrar por sus ocho horas de trabajo, sí, usted, el que me está leyendo, jornalero, que es usted un jornalero.

El estado de bienestar no incluye la libertad de acceso a todo lo que cumple satisfacciones, o dicho de otra manera, no da deber a la satisfacción de todas las necesidades. La determinación inspirada por un antojo, por humor o por deleite en lo extravangante y original no justifica nunca y de ningún modo que el objeto de deseo deba ser adquirido, ni con buenas ni con malas maneras. Y si alguien quiere cobrarle, usted lo tiene fácil, o le paga o no le paga, coge el producto o no lo coge, no juegue a las permutaciones matemáticas y no obtenga el teorema 'no pagar y sí coger'. Descuídese de frases hechas como la de que nadie se va hacer rico con lo vintage, que si es vintage se ha de regalar, que si uno se lo pasa bien programando encima pretende cobrar; todo eso es puro escepticismo, atrévase a invertir en su sistema, cobre por sus producciones, pague por las que le ofrecen, juegue, la piedra gana a la tijera, la tijera gana al papel y el papel gana a la piedra. Hagan juego, señores, sonrían que ahí están los camarógrafos de Quatrosfera y los redactores del 20minutos que van de safari para capturar al geek más elegante, al nerd más maqueado, al freak más sonriente.

Máquinas de hacer dinero

Capitalización de los sistemas vintage es de lo que les estoy hablando, capitalización en la producción y en el consumo. Aquellos que abanderan la personificación del -ero como amiguero, emesequisero o spectrumero, son los que con más ahínco y empeño debieran promover el comercio interno en sus respectivos sistemas. Tengan en cuenta asuntos como el MSX-One-Chip promovido por la MSX Association o las

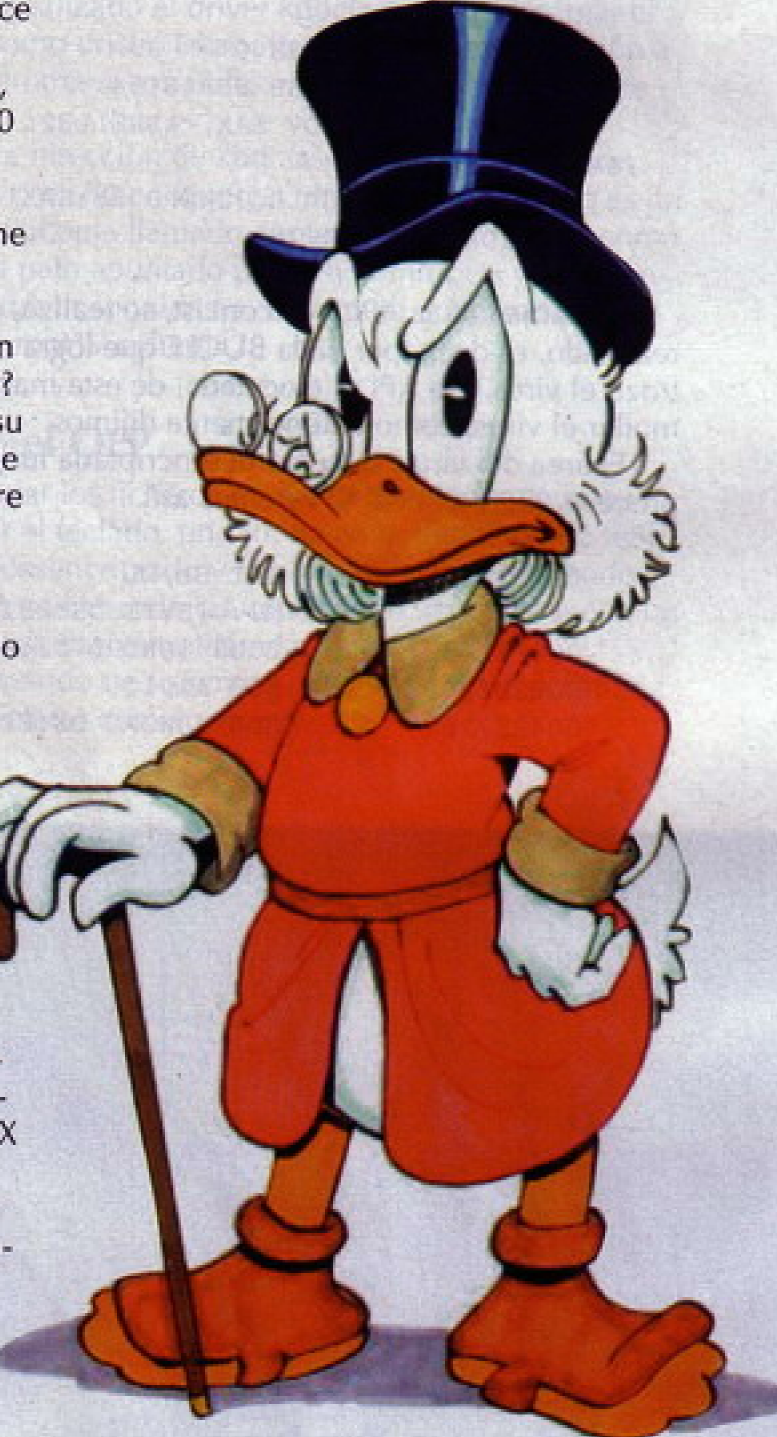
EN 1990 HABÍAN EN ESPAÑA UNOS 20.000 USUARIOS DE AMIGA

Atari Flash Back de la en otro tiempo Infogrames. En este segundo caso la evidencia canta más que una almeja, han comercializado a nivel mundial revisiones de la máquina emblema de Atari, la VCS 2600, un chisme con treinta años a sus espaldas, y ahora anuncian una tercera venida en formato portátil. Quizá no lo sepan pero la actual Atari puso el ojo en foros y sites y viendo la cantidad impresionante de seguidores y de su potencial como desarrolladores y consumidores, contrató a unos cuantos para que ejercieran sobre unos proyectos que ellos en independencia ya tenían planteado evolucionar. Gente como el señor Curt Vendel ahora cobra una nómina por hacer lo que antes hacía por entretenimiento, y otros se frotan las patitas ante la reapertura del Atari Program Exchange, que en pocas palabras significa que usted hace juegos en casa para Atari VCS 2600 y la compañía se los compra y les paga, como cuando Microhobby daba 5.000 pesetas por un juego en BASIC pero mejor y más guay.

Porque, vamos a ver ¿qué le supone a usted pagar digamos que 15 euros una vez cada seis meses -en ejemplo de frecuencia de lanzamientos- por un nuevo juego de su plataforma favorita? ¿O que temor puede tener de ofertar su producto por ese mismo precio? Puede estar seguro de que quien se lo compre lo disfrutará, mientras que si lo libera en la red de redes serán muchos los que lo tendrán pero ¿cuántos de ellos lo valorarán como se precia, jugándolo y disfrutándolo? Sea el número que sea, si tanto lo disfrutan ¿por qué no abonarle a usted una cantidad en calderilla por tanto placer proporcionado? De buen nacido es ser agradecido.

Siendo moderno en lo social, me permito añadir que la existencia de producciones domésticas vintage de pago generan algo similar a lo que podríamos llamar empleo. Todas esas producciones expuestas en ferias y eventos del tipo MadriSX & Retro, RetroEuskal o Vintagenarios, pasarse usted por allí y poder adquirir soft y hardware de reciente manufactura como hace años que no ha podido disfrutar, un incentivo enorme para que tales eventos existan y perduren y no se limiten a macro-mercadillos, museos geriátricos y guateques venidos a menos. Ahí sí que veo yo pancartas y jovencitas objeto incitando al consumo de telefonía celular y conexiones de banda ancha codo a codo con asustados vendedores de cintas de cassette, cederrones y cartuchos para sus nostálgicas máquinas de entretenimiento por video.

Sé que no nos vamos a poner de acuerdo, y ni falta que hace. Yo les expongo una teoría y ustedes se la leen. Mándeme ustedes sus teorías y rebátenme la mía, demuéstrenme que estoy equivocado y que lo mejor para cualquier sistema vintage es darlo todo de forma gratuita, métanme por donde amargan los pepinillos toda mi elucubración y humíllenme, por favor, sírvanse de pasearse por www.matranet.net y utilicen las casillas de correo electrónico que encontrarán dispersas por ahí para ponerse en contacto conmigo, escríbanme y díganme cosas del estilo 'oiga, señor S.T.A.R., usted es un pazguato ¡nos está haciendo pensar!', que no cuesta nada ¿saben? Es gratis.



Análisis del virus peacomm.c

Parte II

Buenas a todos los lectores interesados en el arte de los virus. Hoy les traigo uno de los especímenes más interesantes de los últimos tiempos. Veamos de qué se trata, qué trucos y novedades nos harán deleitar el cerebro.

Revisando lo anterior para continuar

Para arreglar los datos en la cabecera PE, sin primero desencriptarla, es difícil pero veríamos los datos encriptados de cualquier forma, lo mejor es ver el virus en acción con Ollydbg, por ejemplo o ir debugeandolo de a poco. ¿nos animamos?, por supuesto que si! Veamos que sucede.

Ni bien empezamos, veremos el llamado a la API "legal":

```
    0040103A        PUSH 0
    0040103C        PUSH 8FF48154
    00401041        MOV EAX,<&SHELL32.
FreeIconList>
    00401046        CALL [DWORD DS:EAX]
    00401048        RETN
```

La llamada a la API FreeIconList, se realiza, por cada XOR realizado, es decir, por cada BUCLE que logra desencriptar un trozo el virus, esa API es ejecutada, de esta manera, se logra camuflar el virus, como anteriormente dijimos.

El área del virus, quedará desencriptada luego del primer proceso, XOR, el cuál lo veremos así:

```
    0042321F          ADC BL,DL
    00423221          MOV [BYTE DS:ESI],AH
    00423223          LODS [DWORD DS:ESI]
    00423224          SUB AL,1C
    00423226          ADD [DWORD DS:EDX-
 2D],44FE4519
    0042322D          PREFIX REP:
    0042322E          ADD EAX,EDI
    00423230           PUSHFD
    00423231           POP SS
    00423232           PUSH ESI
    00423233           RETF
    00423234           AND EBP,[DWORD
DS:EDX+C29CF800]
```

Bien, luego, de seguir mirando el código, veremos que hay algo de "basura", si seguimos debugeando, se producirá una excepción..

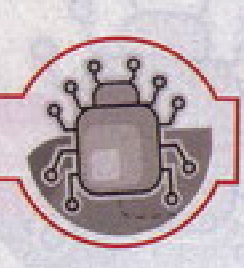
Seguimos mirando un poco más abajo de la dirección 42330d, veremos más instrucciones basura, entonces hay instrucciones como insb/arpl, que son ejecutadas en modo kernel, pero aquí estamos en modo usuario, con lo que no es posible.

Entonces encontramos una instrucción tiene sentido en la dirección 423308, la cuál llama a 423324. Si miramos en forma hexadecimal con el IDA, veremos que se trata de un string.

Luego, de desensamblar correctamente, veremos, a lo largo del virus, que hay variedad de trucos antidebugging.

Desencripción TEA y TIBS Unpacking

Otra parte interesante, que sucede en el virus, es el desencriptado del cuerpo del mismo, una vez pasado el XOR.



```
00423344 sub_423344    proc near               ; CODE XREF: sub_42332A+5↑p
00423346               call    DropSpooldrFilesAndInfect_kbdclassSYS ; 2nd time called infect \drivers\kbdclass.sys
0042334B
0042334B loc_42334B:
0042334B               mov     eax, ss:CounterToCheckIfSpooldrSYSHasAlreadyStartedSpooldrEXE[ebp]
00423351               test    eax, eax
00423353               jz      short InstigateNativeTrojanStart
00423355               call    Call_ExitProcess ; if spooldr.sys has already started spooldr.exe, then exit
0042335A
0042335A InstigateNativeTrojanStart:           ; CODE XREF: sub_423344+0F↑j
0042335A               pop     ebx
0042335B               call    ScanAndImportAllFuncAddressesUsedInTheDecryptedNativeTrojan
00423360               call    Allow_spooldrEXE_at_WindowsFirewall
00423365               pop     edi
00423366               pop     ebx
00423367               pop     esi
00423368               mov     eax, ebp
0042336A               pop     ebp
0042336B               jmp     dword ptr ds:OEP[eax] ; Jump to OEP at 0x40D501
```

Si miramos el volcado con peid, veremós dos signatures de TEA, encontrados, por el programa identificador de PE.

Peid, nos da varias opciones, pero encontramos, en el desensamblado que se trata de TEA, por el DWORD utilizado.

En la imagen de desencripción por TEA, podemos ver, la función principal, que se encuentra en 423F3B.

Como podemos ver, el virus utiliza una clave de 128 bit, en la dirección 426A90. En el registro EDI, tenemos la dirección de los datos a desencriptar.

Por cada sección del ejecutable, se ejecuta el proceso de desencripción de 128 bits.

Luego de finalizar con el proceso de desencripción utilizando TEA, se llama al desempaquetado usando TIBS. Enumera todas las secciones y luego desempaqueta los datos.

El código para desempaquetar entre 4269f7 y 426a6e.

El algoritmo TIBS es un algoritmo de empaquetamiento privado, muy utilizado en malware. Por lo tanto, la mayoría de los Antivirus lo detectan, y existen algoritmos genéricos para detectarlo.

Si no es detectado, esto significa que la engine polimórfica deformó lo suficiente el código para que no sea detectado. Sin embargo, lo siguen detectando de la manera: Trojan:Win32/Tibs.DU.

Files Dropping e Infección de Drivers de Sistema

Después de que el proceso de desencripción y desempaquetado por TIBS, una rutina que se encuentra en 4239DF es llamada, la cuál es la encargada de deshabilitar la protección de ficheros de Windows, en tcpip.sys.

También parchea la función no exportada de la DLL sfc_os.dll, se denomina SfcFileException.

El autor del primer análisis de este virus, sospecha que estas

```
00423F3B TEADecryption1 proc near              ; CODE XREF: TEADecryptionLoop1+6↑p
00423F3B               push    edi
00423F3C               mov     ebx, [edi]      ; ebx <--- edi = start address for decryption
00423F3E               mov     ecx, [edi+4]
00423F41               xor     eax, eax
00423F43               mov     edx, 9E3779B9h  ; delta
00423F48               mov     edi, 20h        ; rounds
00423F4D
00423F4D rotate_32_times_1:                    ; CODE XREF: TEADecryption1+48↓j
00423F4D               add     eax, edx
00423F4F               mov     ebp, ecx
00423F51               shl     ebp, 4
00423F54               add     ebx, ebp
00423F56               mov     ebp, [esi]      ; 1. 32bit value of decryption key
00423F58               xor     ebp, ecx
00423F5A               add     ebx, ebp
00423F5C               mov     ebp, ecx
00423F5E               shr     ebp, 5
00423F61               xor     ebp, eax
00423F63               add     ebx, ebp
00423F65               add     ebx, [esi+4]    ; 2. 32bit value of decryption key
00423F68               mov     ebp, ebx
00423F6A               shl     ebp, 4
00423F6D               add     ecx, ebp
00423F6F               mov     ebp, [esi+8]    ; 3. 32bit value of decryption key
00423F72               xor     ebp, ebx
00423F74               add     ecx, ebp
00423F76               mov     ebp, ebx
00423F78               shr     ebp, 5
00423F7B               xor     ebp, eax
00423F7D               add     ecx, ebp
00423F7F               add     ecx, [esi+0Ch]  ; 4. 32bit value of decryption key
00423F82               dec     edi
00423F83               jnz     short rotate_32_times_1
00423F85               pop     edi
00423F86               mov     [edi], ebx      ; store decrypted bytes on current memory address
00423F88               mov     [edi+4], ecx    ; store decrypted bytes+4 on current memory address
00423F8B               retn
00423F8B TEADecryption1 endp
```

modificaciones posiblemente sean para generar variantes.

Por ejemplo, hay versiones, que parchean la máxima cantidad de conecciones que es típico del malware para realizar DdoS (Ataques de denegación de servicio distribuido). Existen otras versiones que parchean tcpip.sys para cargar el rootkit en spooldr.sys.

En este caso analizado el driver kdbclass.sys para cargar el rootkit spooldr como driver. Estas alternativas como infección a kdbclass.sys y cdrom.sys son útiles, ya que innovan formas de infección.

Después de la infección de kbdclass.sys dos archivos son descomprimidos o dicho en la jerga "dropeados". Primero es un fichero que se autocopia llamado applet.exe y es grabado como spooldr.exe en el path apuntado por %systemroot% y el segundo archivo es el driver spooldr.sys, en el path apuntado por la variable %systemroot%\system32.

Encontrando el OEP

Después de dropear los ficheros e infectar el driver que se encarga de manejar el teclado, una rutina en la dirección 423e5b escanea el virus desencriptado y desempaquetado, buscando sus librerías y los nombres de las funciones. Luego almacena las direcciones de cada función obtenida.

Luego un comando de sistema es ejecutado, para permitir a spooldr.exe conectarse con el exterior.

```
netsh firewall set allowed program
"%systemroot%\spooldr.exe" enable
```

Este comando hace que el firewall permita las conecciones que pueda realizar el fichero spooldr. Por último el JMP final, llama al OEP, en la dirección 403531.

Podemos realizar un dumpeado del virus, simplemente, entrando al OEP apuntando por este último JMP y utilizando el Ollydump para poder realizar el volcado, ahora podremos trabajar con una copia limpia del virus en una máquina virtual.

Recordemos que para poder ejecutar el virus en un entorno seguro, hay que limpiar las detecciones que contiene el virus por si es ejecutado en una máquina virtual, sino seremos infectados.

```
0040314E VirtualPC_IllegalOpcode_Detection:      ; CODE XREF: sub_403389+13↓p
0040314E                 push    14h
00403150                 push    offset stru_420358
00403155                 call    __SEH_prolog
0040315A                 mov     byte ptr [ebp-19h], 0
0040315E                 and     dword ptr [ebp-4], 0
00403162                 push    ebx
00403163                 mov     ebx, 0
00403168                 mov     eax, 1
00403168 ; ---------------------------------------------------------------
0040316D                 db 0Fh, 3Fh, 7, 0Bh     ; Illegal Opcode exception trick
00403171 ; ---------------------------------------------------------------
00403171                 test    ebx, ebx
00403173                 setz    byte ptr [ebp-19h]
00403177                 pop     ebx
00403178                 jmp     short loc_4031AF
0040317A
0040317A ; --------------- S U B R O U T I N E ---------------------------
0040317A
0040317A
0040317A sub_40317A      proc near               ; DATA XREF: .rdata:stru_420358↓o
0040317A                 mov     eax, [ebp-14h]
0040317D                 mov     [ebp-24h], eax
00403180                 mov     eax, [ebp-24h]
00403183                 mov     eax, [eax+4]
00403186                 mov     [ebp-20h], eax
00403189                 mov     eax, [ebp-20h]
0040318C                 or      dword ptr [eax+0A4h], 0FFFFFFFFh
00403193                 mov     eax, [ebp-20h]
00403196                 mov     eax, [eax+0B8h]
0040319C                 add     eax, 4
0040319F                 mov     ecx, [ebp-20h]
004031A2                 mov     [ecx+0B8h], eax
004031A8                 or      eax, 0FFFFFFFFh
004031AB                 retn
004031AB sub_40317A      endp
004031AB
004031AC
004031AC ; --------------- S U B R O U T I N E ---------------------------
004031AC
004031AC
004031AC sub_4031AC      proc near               ; DATA XREF: .rdata:stru_420358↓o
004031AC                 mov     esp, [ebp-18h]
004031AF
004031AF loc_4031AF:                             ; CODE XREF: .text:00403178↑j
004031AF                 or      dword ptr [ebp-4], 0FFFFFFFFh
004031B3                 mov     al, [ebp-19h]
004031B6                 call    __SEH_epilog
004031BB                 retn
004031BB sub_4031AC      endp
```

Parcheando los chequeos por ejecución en VM

Debemos buscar, los chequeos como mencioné antes, y el primero, esta justo después del OEP detectado, en la dirección 403389, llamando a una rutina en 4031bc.

Se trata de una detección usando el ComChannel VMXh, con un número mágico. Esta detección es para VMWARE.

Luego le sigue un chequeo para VirtualPC. Existe un segundo CALL, en la dirección 40339C, saltando hacua 40314E.

Es un truco utilizando un código de operación ilegal.

¿Qué sucede si es detectada una máquina virtual? Exactamente existe un salto a un bucle infinito, "durmiendo" al virus para siempre.

El loop se encuentra en la dirección 403524. La forma de solucionar estos chequeos, es parchear 2 bytes , en la dirección 40338F con un JMP hacia 4033A9.

Analizando el rootkit spooldr

Analizaremos lo mejor que podamos el rootkit mencionado, que forma parte integral del virus.

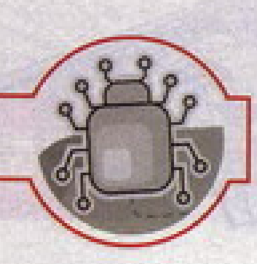
Para empezar, veremos que nos dice el software de chequeo de rootkits y comportamientos anómalos denominado RkUnhooker.

Podremos ver viejo truco, un SSDT hook de una función nativa del SO, llamada NtQueryDirectoryFile.

Más especificamente el CALL de la dirección 177F, realiza el SSDT hook.

Mientras que el primer CALL, inyecta código en el proceso del explorer para iniciar la shellcode que nos llevará hacia el rootkit.

```
    .text:0000175E                    jz
short loc_1785
    .text:00001760                    push
Object                ; Object
    .text:00001766                    call
```



```
sub_1142
    .text:0000176B
push    offset sub_138C ; int
    .text:00001770
push    offset dword_1A54 ;
int
    .text:00001775
push    offset
aZwquerydirec_0 ;
"ZwQueryDirectoryFile"
    .text:0000177A
call    sub_B70
    .text:0000177F
dec     dword_1A5C
    .text:00001785
```

Ahora analizaremos, algo bastante curioso, que hace diferir a este virus, y su rootkit, de muchos vistos hasta hoy en día, por una técnica inusual y muy interesante. Esto sucede cuando se lee bien la documentación de los SO, API's, programación de drivers a fondo, entre otras cosas. :)

```
    .text:000018F9
call    sub_110C
```

Esta función de aquí arriba, se ejecuta al comienzo del rootkit, y es simplemente un algoritmo de notificación del rootkit. Si algun Antivirus, o módulo de algún Antivirus, está cargado en memoria y está abriendo el proceso del rootkit, este, se parchea a sí mismo, simulando un código que hace que termine el análisis rápido, sin llegar al corazón del rootkit.

Utiliza la función PsSetLoadImageNotifyRoutine, y sirve justamente, como en su definición dice, para notificar, cuando una imagen binaria es abierta para su ejecución.

Por lo tanto, el virus sabe cuando su rootkit, se empezará a analizar, con lo cuál, se parchea a sí mismo y termina el proceso, para evitar ser detectado.

Es, simplemente, una obra de arte.

```
004031BC VMWare_ComChannel_VMXh_Magic_Detection proc near ; CODE XI
004031BC
004031BC var_19          = byte ptr -19h
004031BC ms_exc          = CPPEH_RECORD ptr -18h
004031BC
004031BC                 push    0Ch
004031BE                 push    offset stru_420368
004031C3                 call    __SEH_prolog
004031C8                 mov     [ebp+var_19], 1
004031CC                 and     [ebp+ms_exc.disabled], 0
004031D0                 push    edx
004031D1                 push    ecx
004031D2                 push    ebx
004031D3                 mov     eax, 'VMXh'
004031D8                 mov     ebx, 0
004031DD                 mov     ecx, 0Ah
004031E2                 mov     edx, 'VX'
004031E7                 in      eax, dx
004031E8                 cmp     ebx, 'VMXh'
004031EE                 setz    [ebp+var_19]
004031F2                 pop     ebx
004031F3                 pop     ecx
004031F4                 pop     edx
004031F5                 jmp     short loc_403202
004031F7 ;
004031F7
004031F7 loc_4031F7:                             ; DATA XREF: .rdat
004031F7                 xor     eax, eax
004031F9                 inc     eax
004031FA                 retn
004031FB ;
004031FB
004031FB loc_4031FB:                             ; DATA XREF: .rdat
004031FB                 mov     esp, [ebp+ms_exc.old_esp]
004031FE                 mov     [ebp+var_19], 0
00403202
00403202 loc_403202:                             ; CODE XREF: VMWar
00403202                 or      [ebp+ms_exc.disabled], 0FFFFFFFFh
00403206                 mov     al, [ebp+var_19]
00403209                 call    __SEH_epilog
0040320E                 retn
0040320E VMWare_ComChannel_VMXh_Magic_Detection endp
```

Conclusión

Bien amigos, estamos llegando a lo mejor, lo veremos en el próximo número. Como se parchea a sí mismo, como termina el proceso, y como el Antivurus (AV) es engañado. Realmente una forma de evadir las engines, sumando todas sus características ya vistas, propias de una obra de arte. Algo así, como un rompecabezas, hecho de adentro hacia afuera, donde todas sus partes encajan a la perfección.

Espero que lo estén disfrutando tanto como yo...

Nos vemos en la próxima.

SparK
http://www.disidents.org
http://www.intrabytes.com
spark@disidents.org

arquitectura de computadores

La unidad de control (III)

A pesar de ser, dentro de las disciplinas implicadas, una de las más importantes, la electrónica (en este caso, electrónica digital) no lo es todo en el diseño de computadores. Cuando de elementos complejos se trata, como es el caso de la unidad de control, las abstracciones matemáticas pueden ser de gran ayuda para comprender, modelar y optimizar el diseño de los mismos. Así, a la hora de trabajar con unidades de control cableadas, resulta muy útil echar mano de los modelos matemáticos estudiados por la disciplina de la teoría de autómatas.

Hola una vez más a todos, desde el rincón de la arquitectura de computadores. El mes pasado estudiamos ciertos elementos de vital importancia -desde el punto de vista de la electrónica- para el diseño de sistemas digitales, como son el buffer y el registro. Tras comprender las circunstancias que hacen necesaria su existencia, así como sus particularidades, diseño e implementación; vimos cómo podríamos usar ambos elementos para construir un sistema muy básico de memoria.

Si probasteis a jugar con el sistema diseñado en el simulador Vsystem, habréis observado la vital importancia que toman los tiempos, del orden de los nanosegundos, en este tipo de componentes. Como consecuencia de la gran cantidad de elementos puestos en juego, y de los requisitos de precisión en los tiempos, la sincronización se convierte en una tarea harto compleja. Dicha complejidad hace que resulte especialmente útil ayudarse de determinados modelos matemáticos para diseñar estos elementos.

Modelando un sistema

Vamos con uno de esos ejercicios mentales que tanto me gustan. Imaginemos una hipotética unidad de control que recibe la siguiente instrucción en ensamblador:

```
ADD R1,R2
```

Esta instrucción tomaría los datos contenidos en los registros R1 y R2, efectuaría sobre ellos la operación de suma, y finalmente dejaría el resultado en el registro R1. Ahora consideraremos un concepto llamado "estado interno", que determina qué está teniendo lugar en el interior de la unidad de control en un instante de tiempo concreto. Según los datos recibidos por la unidad de control, este estado variará entre una serie de posibilidades.

Veamos cómo se aplicaría ésto a la instrucción propuesta:

- Estado "inicial", recibe código de operación "ADD".
- Estado "suma", recibe operando "R1".

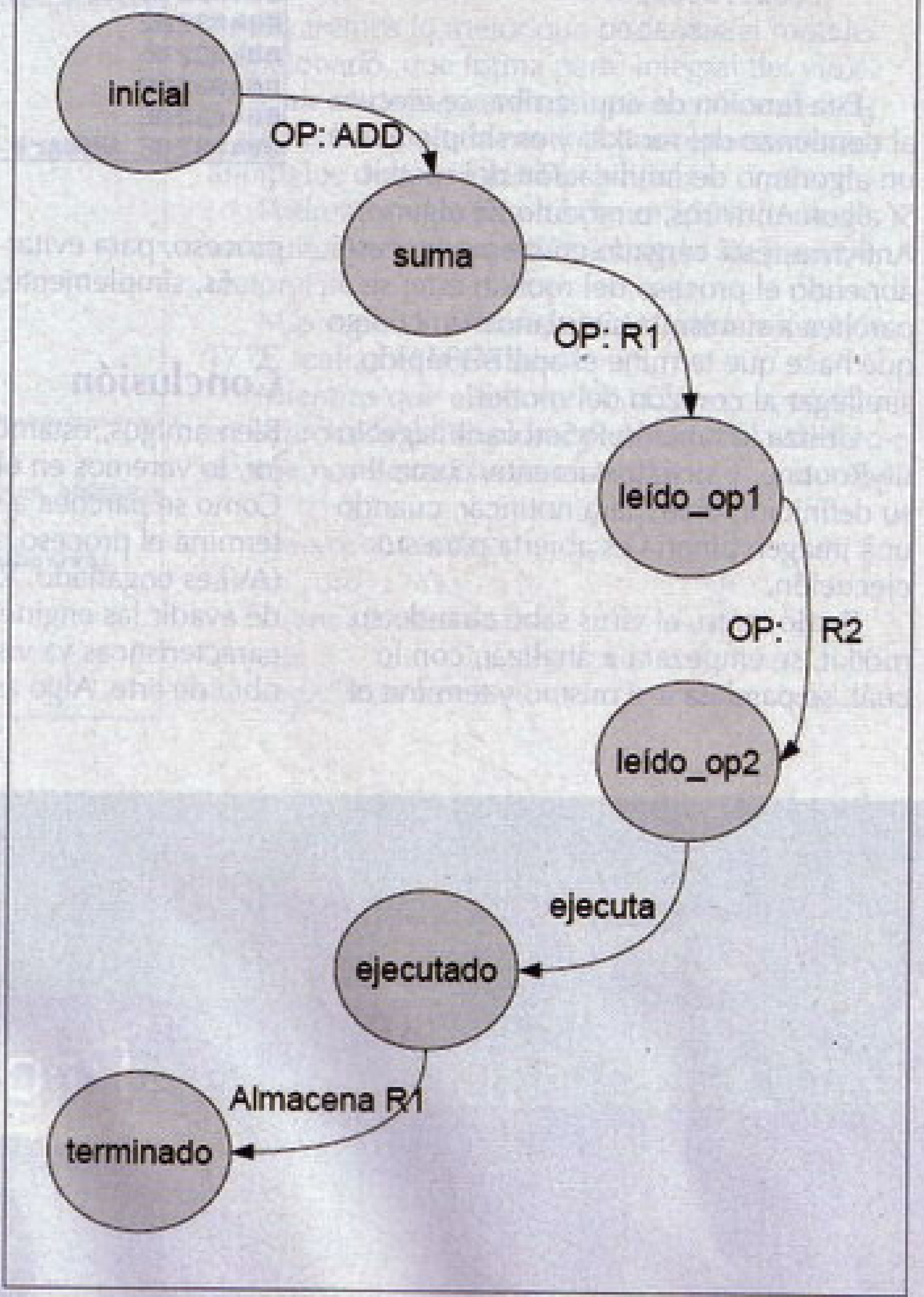
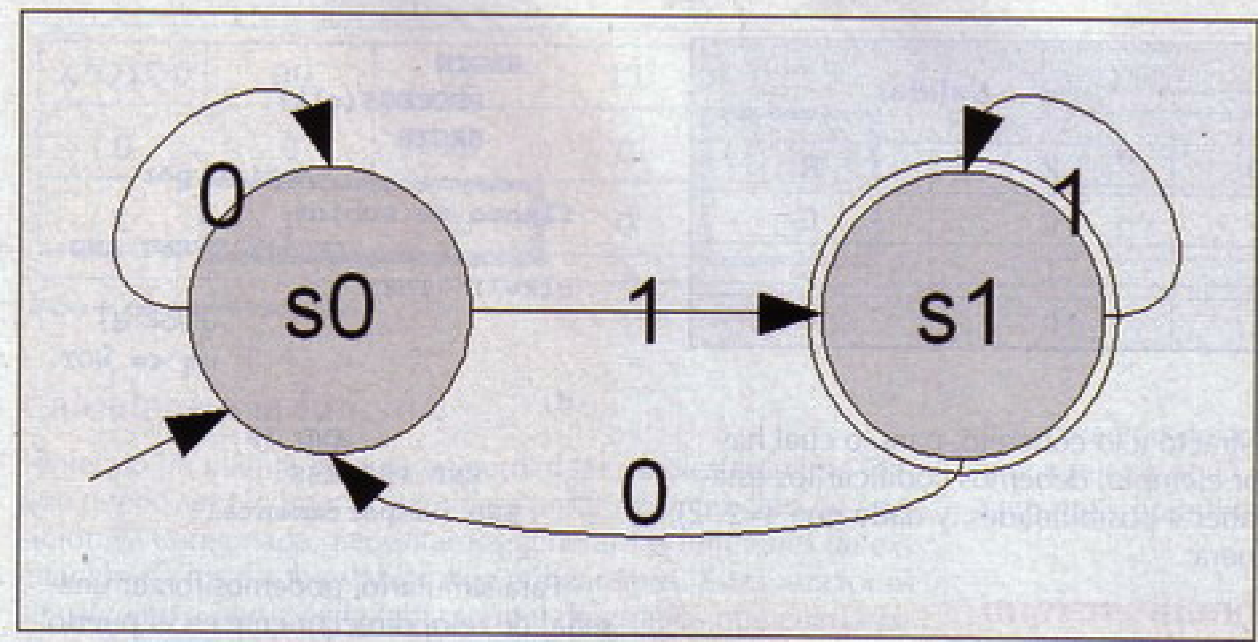


Diagrama de esados para la operación ADD.





Ejemplo de autómata finito.

• Estado "leído_op1", recibe operando "R2".
• Estado "leído_op2", ejecuta la operación.
• Estado "ejecutado", escribe resultado en "R1".
• Estado "terminado".

Máquinas de estados

Así, el funcionamiento de la unidad de control podría ser representado por todos los posibles estados internos de la misma, así como las transiciones entre ellas según las distintas entradas que reciba. A esta abstracción se la denomina máquina de estados finita, y una unidad de control cableada no es más que una de estas máquinas, si bien de una complejidad muy, muy elevada.

A su vez, estas máquinas de estados son un caso particular de los denominados autómatas finitos, cuyo estudio corresponde a la disciplina de la teoría de autómatas y lenguajes formales. Un autómata sencillo sería el siguiente.

Este autómata tiene dos estados, que representan si el último dato recibido es un cero o un uno. Al recibir un cero como entrada, el autómata pasa al estado s0; mientras que si recibe un uno, pasará a s1. Dado que el estado aceptador es s1, este autómata aceptará las cadenas terminadas en uno. Se trata de un ejemplo muy, muy sencillo (el más simple que se me ha ocurrido), pero os aseguro que se puede complicar hasta la saciedad; y de hecho en ingeniería, suele existir una asignatura para estudiar de forma exclusiva los autómatas.

EL FUNCIONAMIENTO DE LA UNIDAD DE CONTROL PODRÍA SER REPRESENTADO POR TODOS LOS POSIBLES ESTADOS INTERNOS DE LA MISMA, ASÍ COMO LAS TRANSICIONES ENTRE ELLAS SEGÚN LAS DISTINTAS ENTRADAS QUE RECIBA

Nuestra máquina de estados

Vamos a imaginarnos una máquina de estados muy sencilla, y a ver cómo se implementaría mediante componentes electrónicos digitales como los que hemos venido utilizando hasta ahora, para poder hacernos una idea de cómo se podrían modelar unidades de control reales. Nuestra máquina de estados será la siguiente: (ver figura)

Las salidas asociadas a cada estado son las siguientes: (ver figura)

Nuestra máquina de estados.

El diseño tiene únicamente cuatro estados, y se describen las excitaciones externas que debe recibir el sistema para cambiar de estado. Para el estado inicial A, un "1" lógico hará que el sistema comience el proceso, pasando al estado B. Cuando el sistema se encuentra en el estado B, requiere un "0" lógico para pasar al tercer estado. La transición del estado C al estado D se da para cualquier valor de entrada, "0" ó "1", lo cual suele denominarse "DC" (del inglés "Don't Care"). Una vez en el estado final D (el cual se correspondería al estado aceptador del autómata, aunque no haya sido representado), cualquier entrada hará que el sistema se sitúe en el estado inicial nuevamente.

Resumiendo el comportamiento descrito junto a las salidas asociadas, en una sola tabla, obtenemos lo siguiente:

Estados	Salidas	
	Z	R
A	0	0
B	1	0
C	0	0
D	0	1

Tabla de salidas para cada estado.

Estado actual	Estado sucesor		Salidas	
	X=0	X=1		
Q1Q0	Q1Q0	Q1Q0	Z	R
0 0	0 0	0 1	0	0
0 1	1 0	0 1	1	0
1 0	1 1	1 1	0	0

Tabla informal de estados.

Ha llegado el momento de pasar de lo abstracto a lo concreto, para lo cual hay que empezar a pensar en señales digitales. Por ejemplo, debemos codificar los estados, para lo cual necesitaremos dos bits (al haber 4 posibilidades, y dado que 4=2^2). Codificaremos los estados de la siguiente manera:

```
A = 00
B = 01
C = 10
D = 11
```

Estado actual	Estado sucesor		Salidas	
	Entrada = 0	Entrada = 1	Z	R
A	A	B	0	0
B	C	B	1	0
C	D	D	0	0
D	A	A	0	1

Tabla formal de estados.

El biestable D

Si echáis un vistazo a entregas anteriores, recordaréis que en su momento (en la séptima entrega) hablamos de circuitos combinacionales y secuenciales. Son éstos últimos precisamente los que resultarán útiles para diseñar elementos que, como nuestra simulación, necesiten de estados en su ejecución.

Ya entonces hablamos también de los circuitos biestables, multivibradores capaces de mantener un estado de salida estable durante tiempo indefinido. Concretamente, realizamos la implementación estructural de un biestable tipo RS con puertas NOR, y de un biestable de tipo JK con puertas NAND. Ahora, y para no utilizar estos mismos, vamos a trabajar con un biestable de tipo D.

El biestable de tipo D es, posiblemente, el más sencillo de los biestables. Posee una única entrada de datos D (además del reloj, al ser un circuito síncrono) y dos salidas (Q y noQ), y su comportamiento es el siguiente: la salida positiva (Q) sigue el valor de entrada D, mientras que la salida negativa (noQ) posee el valor contrario. De esta forma, su función de transición sería la siguiente:

```
Q(t+1) = D(t)
noQ(t+1) = NOT D(t)
```

Implementaremos este circuito de forma comportamental, para evitar los posibles problemas de oscilaciones ocasionados por la realimentación de puertas lógicas. La implementación del biestable sería la siguiente:

```
ENTITY ffD IS
   PORT (d,clk: IN BIT;
         q,nq: INOUT BIT);
END ffD;

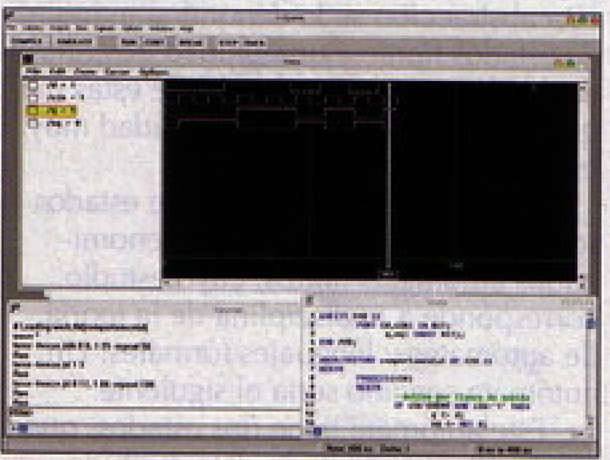
ARCHITECTURE comportamental OF ffD IS
```

```
BEGIN
   PROCESS(clk)
   BEGIN
         --Activo por
flanco de subida
         IF clk'EVENT AND
clk='1' THEN
               q <= d;
               nq <= NOT
d;
         END IF;
   END PROCESS;
END comportamental;
```

Para simularlo, podemos forzar una señal de reloj directamente en el puerto de entrada del componente, sin necesidad de cargar un reloj externo. Para ello, utilizaremos la opción "force signal" en modo "freeze" con valor de 0 con retraso 0 ns, valor de 1 con retraso 25 ns, y repetición activa cada 50 ns. Otra forma de realizar esta misma operación es mediante la siguiente orden ejecutada en la ventana de transcript:

```
force -freeze /clk 0 0, 1
25 -repeat 50
```

Podemos ver un ejemplo de la salida de este tipo de biestables en la siguiente simulación:



Simulación del biestable tipo D.

EL BIESTABLE DE TIPO D ES, POSIBLEMENTE, EL MÁS SENCILLO DE LOS BIESTABLES



X/Q1Q0	00	01	11	10
0	0	0	0	1
1	1	1	0	1

X/Q1Q0	00	01	11	10
0	0	1	0	1
0	0	0	0	1

Mapas de Karnaugh de los circuitos.

Calculando la función

Teniendo en cuenta la tabla de verdad de un biestable tipo D, que puede ser fácilmente inferida a partir de la función de transición ya comentada, necesitamos generar las funciones de excitación de los dos biestables que utilizaremos. Estas funciones se calculan a partir de la tabla formal de estados que encontrarás junto a estas líneas.

Por motivos prácticos, y para evitar generar circuitos con un número excesivo de puertas, realizaré la simplificación de estas funciones mediante la técnica de los mapas de Karnaugh. No es necesario comprender este paso, y no lo explicaré porque se sale demasiado de los objetivos de este curso, pero os animo a que investiguéis por la red sobre el tema, porque puede resultar muy útil e interesante.

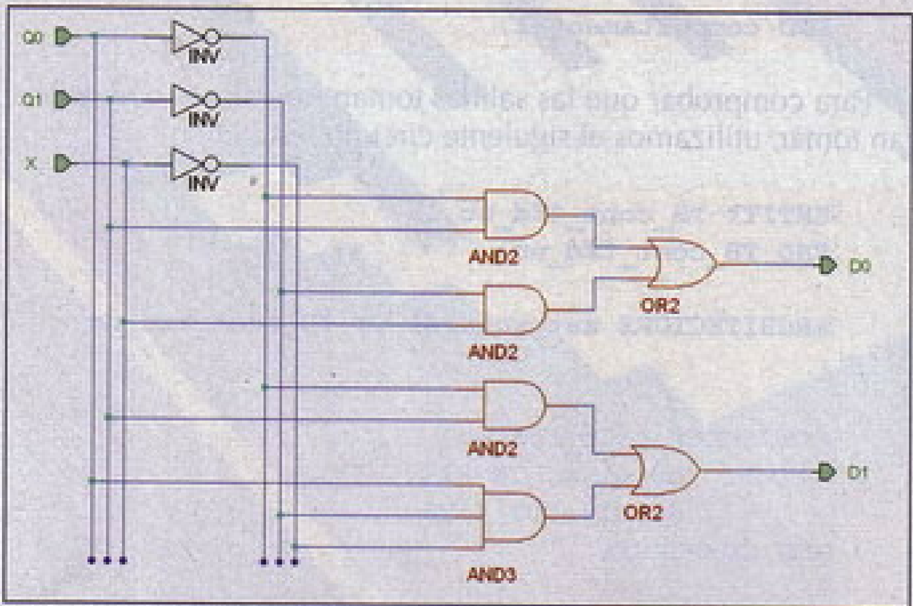
Las funciones de excitación quedarían de la siguiente forma:

```
    D0 = ((NOT QO) AND Q1) OR ((NOT Q1) AND X)
    D1 = ((NOT Q0) AND Q1) OR (Q0 AND (NOT Q1)
AND (NOT X))
```

O, expresándolas de forma abreviada:

```
    D0 = !Q0·Q1 + !Q1·X
    D1 = !Q0·Q1 + Q0·!Q1·!X
```

Debemos diseñar un circuito combinacional que genere estas dos señales de excitación para los biestables del sistema. Una propuesta de diseño sería la siguiente:



Diseño de la lógica para la unidad de contro.

Sería posible realizar otros diseños, y de hecho es muy fácil eliminar una de las puertas AND, pues la función parcial "((NOT QO) AND Q1)" se usa en ambas salidas, y podría obtenerse de una única puerta, pero para que quede más clara la separación de ambas señales, he preferido "malgastar" una única puerta AND más, sabiendo además que el cálculo es concurrente y no influirá en la velocidad de cómputo.

Implementando el controlador lógico

Una vez tenemos la función lógica que deberá calcular el controlador, y con un diseño realizado, sólo queda implementarlo en código VHDL. Para variar, y por explorar nuevas posibilidades del lenguaje, vamos a realizar dos implementaciones -estructural y comportamental- del controlador en una única entidad.

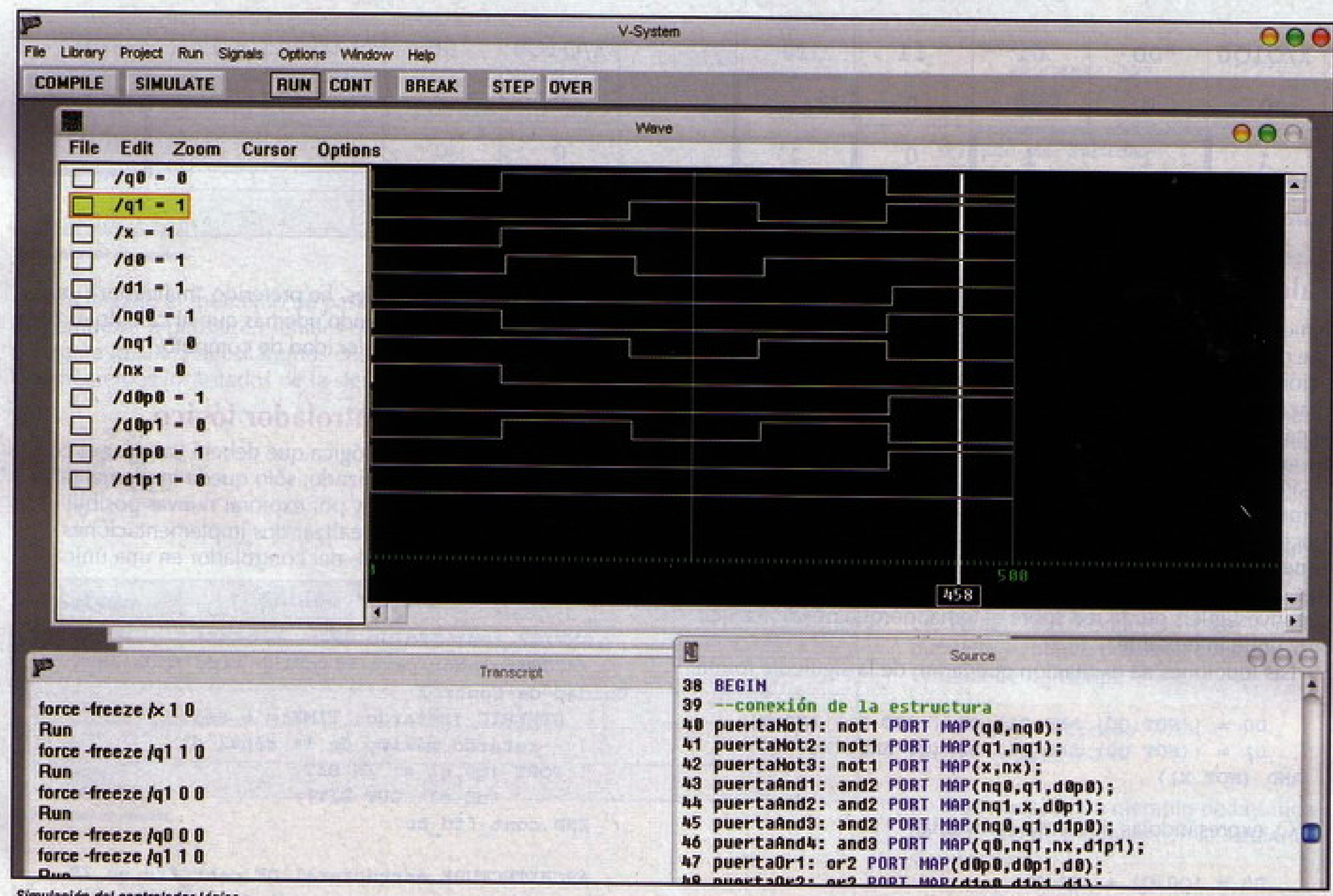
```
   ENTITY cont_ffd_uc IS
   --CONTrolador para FlipFlop tipo D de la
Unidad de Control
     GENERIC (retardo: TIME:= 6 ns);
     --retardo máximo de la señal d1
     PORT (q0,q1,x: IN BIT;
           d0,d1: OUT BIT);
   END cont_ffd_uc;

   ARCHITECTURE estructural OF cont_ffd_uc IS
   --Arquitectura estructural del controlador

   --declaración de componentes
   COMPONENT not1
     PORT (a: IN BIT; z: OUT BIT);
   END COMPONENT;
   COMPONENT and2
     PORT (a,b: IN BIT; z: OUT BIT);
   END COMPONENT;
   COMPONENT and3
     PORT (a,b,c: IN BIT; z: OUT BIT);
   END COMPONENT;
   COMPONENT or2
     PORT (a,b: IN BIT; z: OUT BIT);
   END COMPONENT;

   --declaración de señales
   SIGNAL --niveles iniciales negados
          nq0, nq1, nx,
          --salidas del primer nivel de puertas
          d0p0, d0p1, d1p0, d1p1: BIT;

   --ubicación de arquitecturas
   FOR ALL: not1 USE ENTITY WORK.
not1(comportamental);
   FOR ALL: and2 USE ENTITY WORK.
and2(comportamental);
   FOR ALL: and3 USE ENTITY WORK.
and3(comportamental);
```



Simulación del controlador lógico.

```
   FOR ALL: or2 USE ENTITY WORK.
or2(comportamental);

   BEGIN
   --conexión de la estructura
   puertaNot1: not1 PORT MAP(q0,nq0);
   puertaNot2: not1 PORT MAP(q1,nq1);
   puertaNot3: not1 PORT MAP(x,nx);
   puertaAnd1: and2 PORT MAP(nq0,q1,d0p0);
   puertaAnd2: and2 PORT MAP(nq1,x,d0p1);
   puertaAnd3: and2 PORT MAP(nq0,q1,d1p0);
   puertaAnd4: and3 PORT MAP(q0,nq1,nx,d1p1);
   puertaOr1: or2 PORT MAP(d0p0,d0p1,d0);
   puertaOr2: or2 PORT MAP(d1p0,d1p1,d1);

   END estructural;

   ARCHITECTURE comportamental OF cont_ffd_uc
IS
   --Arquitectura comportamental del
controlador
   BEGIN

   d0<=((NOT q0) AND q1) OR ((NOT q1) AND x)
AFTER retardo;
   d1<=((NOT q0) AND q1) OR ((NOT q1) AND (NOT
x) AND q0) AFTER retardo;

   END comportamental;
```

Para comprobar que las salidas toman los valores que deberían tomar, utilizamos el siguiente circuito test bench:

```
   ENTITY TB_cont_ffd_uc IS
   END TB_cont_ffd_uc;

   ARCHITECTURE estructural OF TB_cont_ffd_uc
IS

   COMPONENT cont_ffd_uc
     PORT (q0,q1,x: IN BIT;
          d0,d1: OUT BIT);
   END COMPONENT;

   FOR ALL: cont_ffd_uc USE ENTITY WORK.cont_
ffd_uc(estructural);

   SIGNAL q0,q1,x,d0,d1: BIT;

   BEGIN
```



```
        controlador: cont_ffd_uc PORT
MAP(q0,q1,x,d0,d1);

        PROCESS
        BEGIN

                q0 <= '0';
                q1 <= '0';
                x  <= '0';
                WAIT FOR 30 ns;
                --Valores teóricos: d0=0 ; d1=0
                q0 <= '1';
                q1 <= '0';
                x  <= '1';
                WAIT FOR 30 ns;
                --Valores teóricos: d0=1 ; d1=0
                q0 <= '1';
                q1 <= '1';
                x  <= '1';
                WAIT FOR 30 ns;
                --Valores teóricos: d0=0 ; d1=0
                q0 <= '0';
                q1 <= '1';
                x  <= '1';
                WAIT FOR 30 ns;
                --Valores teóricos: d0=1 ; d1=1

        END PROCESS;

    END estructural;
```

El mes que viene...

Ahora que disponemos del controlador lógico que hará operar nuestra máquina de estados, nos queda unir éste a los biestables tipo D, y dicho conjunto a las puertas lógicas que generarán la salida. Todo ello, junto a un reloj que gobernará el sincronismo del circuito, constituirá la máquina de estados. Hasta el mes que viene, os animo a que intentéis pensar cómo se realizarían estos pasos.

Como todos los meses, os recuerdo que mi correo está disponible para aquellos que deseen consultar dudas o cuestiones relacionadas con el curso, y que el código fuente desarrollado hasta ahora en el curso está disponible en mi blog personal, en la sección de artículos.

¡Hasta el mes que viene!

Ramiro Cano Gómez
death_master@hpn-sec.net
http://omniumpotentior.wordpress.com/

criptografía asimétrica

PARTE III

Hoy regresamos, analizando y repasando lo visto en el número anterior, agregando el tema de firmas digitales, que dimos un primer paso y ahora continuaremos explicando y definiendo varios aspectos.

Repasando

Para los olvidadizos, esta es la parte, donde recordarán que estábamos viendo un programa ejemplo, que generaba, las llaves, y hacía el proceso de encripción y desencripción utilizando la conocida criptografía asimétrica.

```
1.byte[] _bytKey =
(Rijndael.Create()).Key;
2.byte[] _
bytEncriptadoSimetrico =
MiRijndael.Encriptar(TEXTO
QUE QUIERO ENCRIPTAR, _
bytKey);
```

Bien, luego aquí arriba, en la línea 1, se declara la memoria para almacenar la llave utilizada por nuestro Rijndael personalizado y en la línea 2, se encripta el texto y se obtiene la llave que se utilizó para la encriptación

```
1.byte[] _
bytEncriptadoLlave = _
objEncriptadorPublico.
Encrypt(_bytKey, false);
2._bytEncriptado
= new byte[_
bytEncriptadoLlave.Length
+ _bytEncriptadoSimetrico.
Length];
3._bytEncriptadoLlave.
CopyTo(_bytEncriptado,0);
4._
bytEncriptadoSimetrico.
CopyTo(_bytEncriptado, _
bytEncriptadoLlave.Length);
```

Luego en este trozo de código, en la línea 1, se encripta la llave con el algoritmo RSA y en las líneas 2 y 3, se copia en un arreglo la llave encriptada y el encriptado de Rijndael.

```
1.this._objKey.
DesEncriptar(_
bytEncriptado);
```

Para desencriptar se utiliza el arreglo de bytes obtenido mas arriba. Esta función no debiera ser pública. Sólo lo es acá para explicarlo mejor.

Planteamiento de Casos

1° caso: cuando un usuario, A, quiere enviar información a otro usuario, B, utiliza la clave pública de B (KpuB) para encriptar los datos.

El usuario B utilizará su clave privada (que sólo él conoce)(KprB) para obtener el texto en claro a partir de la información (encriptada) recibida. Si otro usuario, C, quiere enviar información al usuario B, también empleará la clave pública (KpuB) .

Este modo se puede emplear para proporcionar el servicio de confidencialidad, porque sólo el usuario B es capaz de descifrar los mensajes que los usuarios A y C le han enviado.

2° caso: es el usuario B quien encripta la información utilizando su clave privada, (KprB) de forma que cualquiera que conozca (KpuB) podrá descifrar la información transmitida.

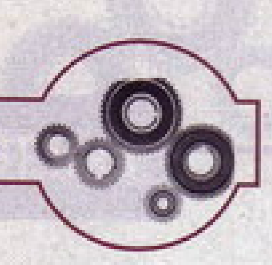
De esta forma se puede emplear para proporcionar el servicio de autenticación, ya que la obtención del texto en claro a partir del texto cifrado es una garantía de que el emisor del mensaje es el propietario de (KpuB) (lógicamente, para saber que el mensaje obtenido de la desencriptación del texto cifrado es el texto en claro original, éste se ha de obtener por otros medios para realizar la comparación).

Esto es la base de las firmas digitales

La firma digital es el instrumento que va a permitir (entre otras cosas), determinar de forma fiable si las partes que intervienen en una transacción, son realmente las que dicen ser, y si el contenido del contrato ha sido alterado o no posteriormente.

Podemos definirlo también como un conjunto de datos asociados a un mensaje que permite asegurar la identidad del firmante y la integridad del mensaje.

EN JURISDICCIONES DE TODO EL MUNDO, LAS FIRMAS DIGITALES GANAN GRADUALMENTE, A TRAVÉS DE MEDIOS LEGALES, EL MISMO PESO LEGAL QUE LA FIRMA MANUSCRITA



Que utilicemos firma digital no significa que el mensaje esté encriptado, sino que; al igual que cuando se firma un documento holográficamente, este puede ser visto por otras personas.

Las utilidades que posee la firma digital pueden ser muchísimas, algunas mencionadas son:

- Mensajes sin posibilidad de repudio
- Contratos comerciales electrónicos
- Factura_Electrónica
- Desmaterialización de documentos
- Transacciones comerciales electrónicas
- Invitación electrónica
- Dinero electrónico
- Notificaciones judiciales electrónicas
- Voto electrónico
- Decretos ejecutivos (gobierno)
- Créditos de seguridad social
- Contratación pública
- Sellado de tiempo
- Mensajes con autenticidad asegurada

Existen varios tipos de firmas digitales:

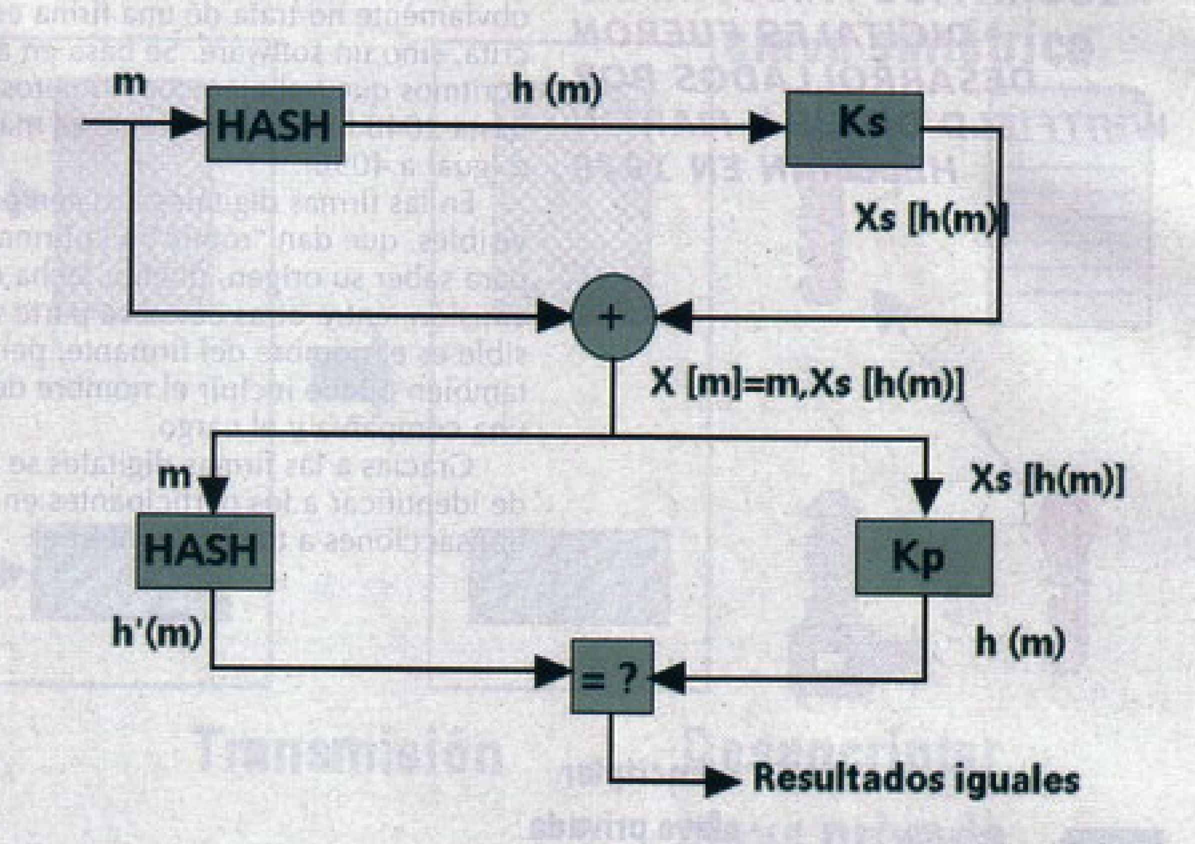
- **Firma básica:** Incluye el resultado de operación de hash y clave privada, identificando los algoritmos utilizados y el certificado asociado a la clave privada del firmante. A su vez puede ser "attached" o "detached", "enveloped" y "enveloping".
- **Firma fechada:** A la firma básica se añade un sello de tiempo calculado a partir del hash del documento firmado por una TSA (Time Stamping Authority).
- **Firma validada o firma completa:** A la firma fechada se añade información sobre la validez del certificado procedente de una consulta de CRL o de OCSP realizada a la Autoridad de Certificación.

Importancia en el mundo real

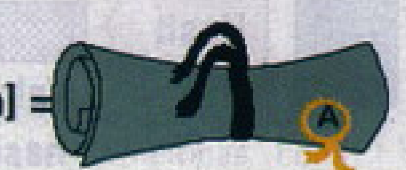
En jurisdicciones de todo el mundo, las firmas digitales ganan gradualmente, a través de medios legales, el mismo peso legal que la firma manuscrita. Hay un gran esfuerzo por parte de los gobiernos para "oficializar" la firma digital, como medio autorizante.

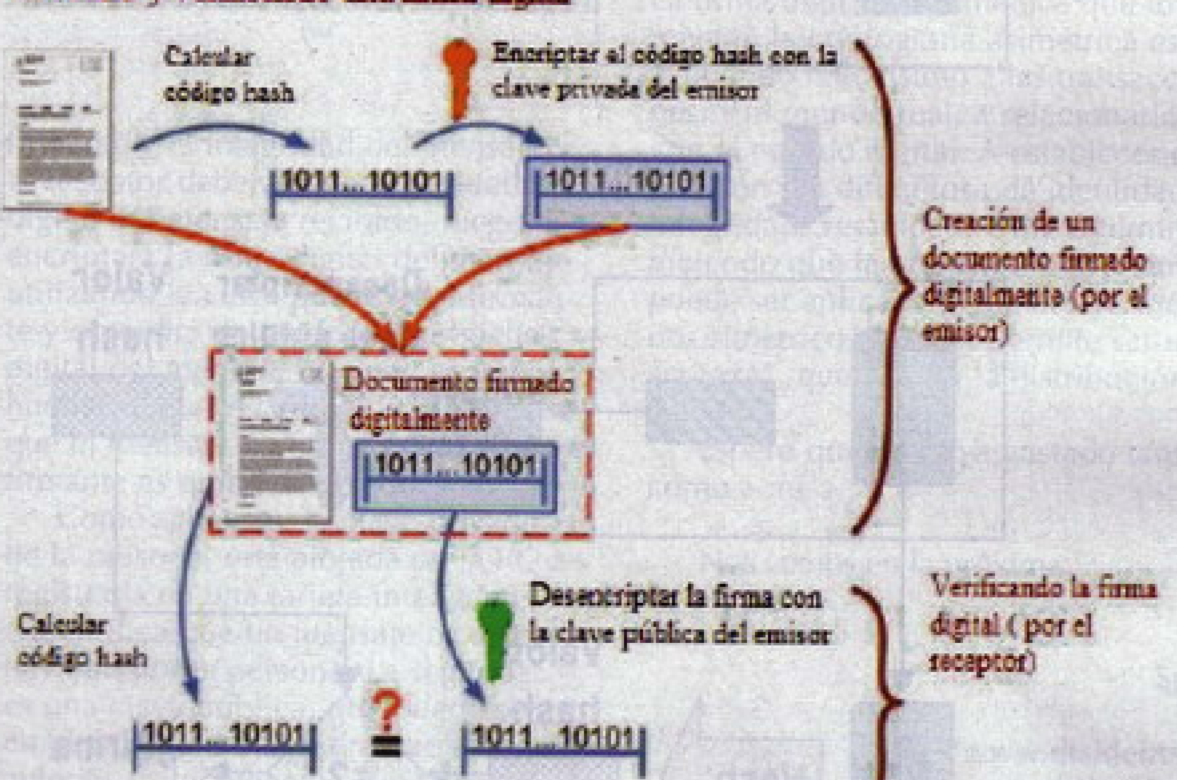
La Firma Digital es, sin duda, una manera segura de firmar un documento electrónico como cartas, contratos o trabajos.

Además, nos brinda la garantía de que el mensaje procede en realidad del remitente, que no ha sido interve-



Firma de usuario A representada por: X[m] =





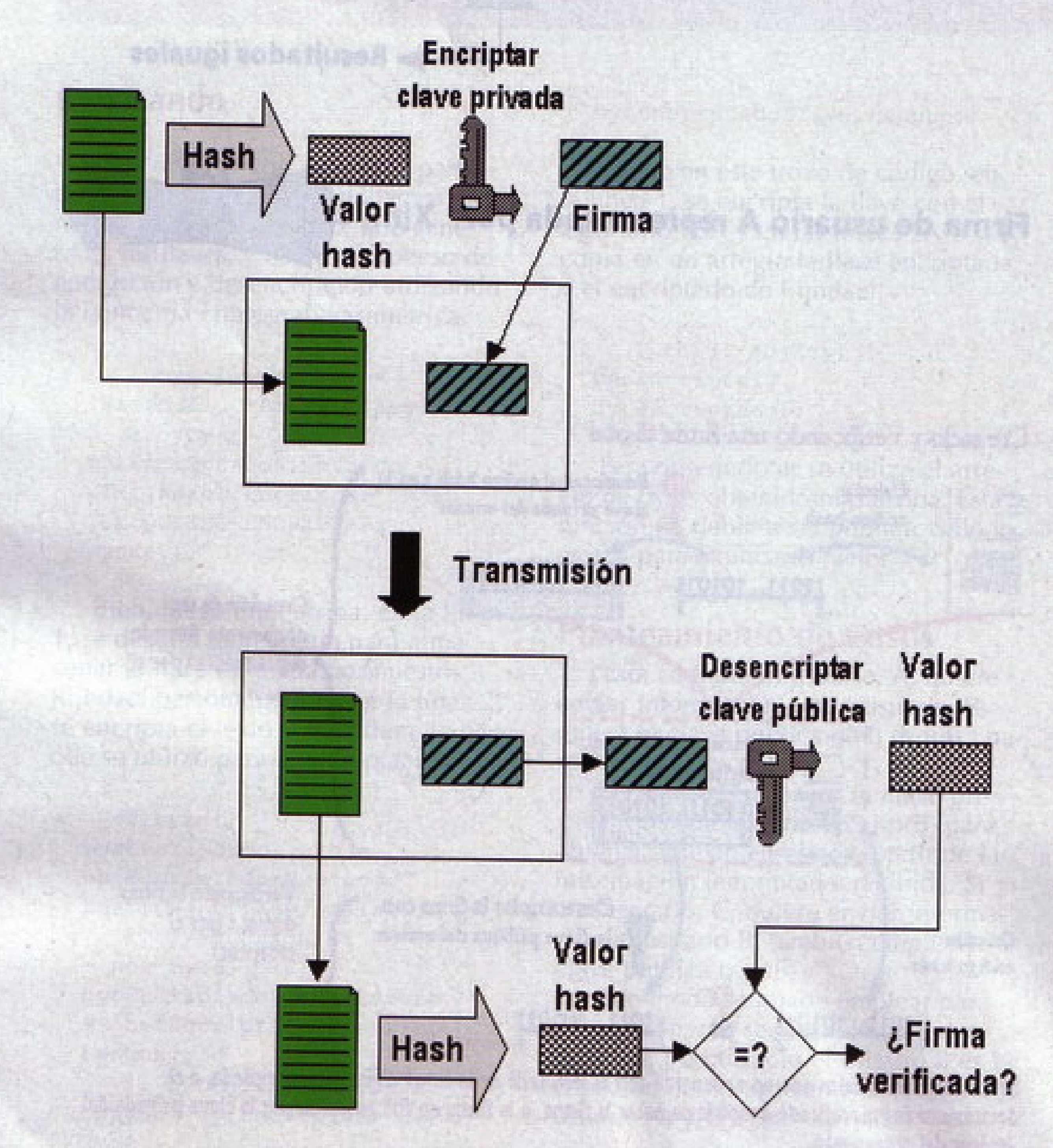
LOS PRIMEROS ALGORITMOS PARA FIRMAS DIGITALES FUERON DESARROLLADOS POR WHITFIELD DIFFIE Y MARTIN HELLMAN EN 1976

nido y que aquél es quien dice ser.

Como ya muchos pueden imaginar, obviamente no trata de una firma escrita, sino un software. Se basa en algoritmos que trabajan con números de hasta 2048 bits (militarmente es mayor o igual a 4096).

En las firmas digitales, existen partes visibles, que dan "rótulo" a la firma, para saber su origen, dueño, fecha de emisión, entre otras cosas.La parte visible es el nombre del firmante, pero también puede incluir el nombre de una compañía y el cargo.

Gracias a las firmas digitales se puede identificar a los participantes en las transacciones a través de Internet.



Origen de las firmas digitales

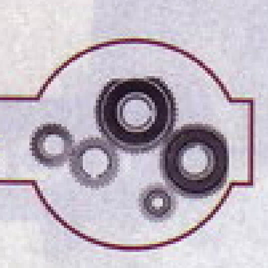
Los primeros algoritmos fueron desarrollados por Whitfield Diffie y Martin Hellman en 1976 (por si no recuerdan, el algoritmo diffie-hellman). Los más populares son el RSA, de 1977 (por las iniciales de Ron Rivest, Adi Shamir y Leonard Adleman, sus inventores), incluido en el Internet Explorer y el Netscape Navigator.

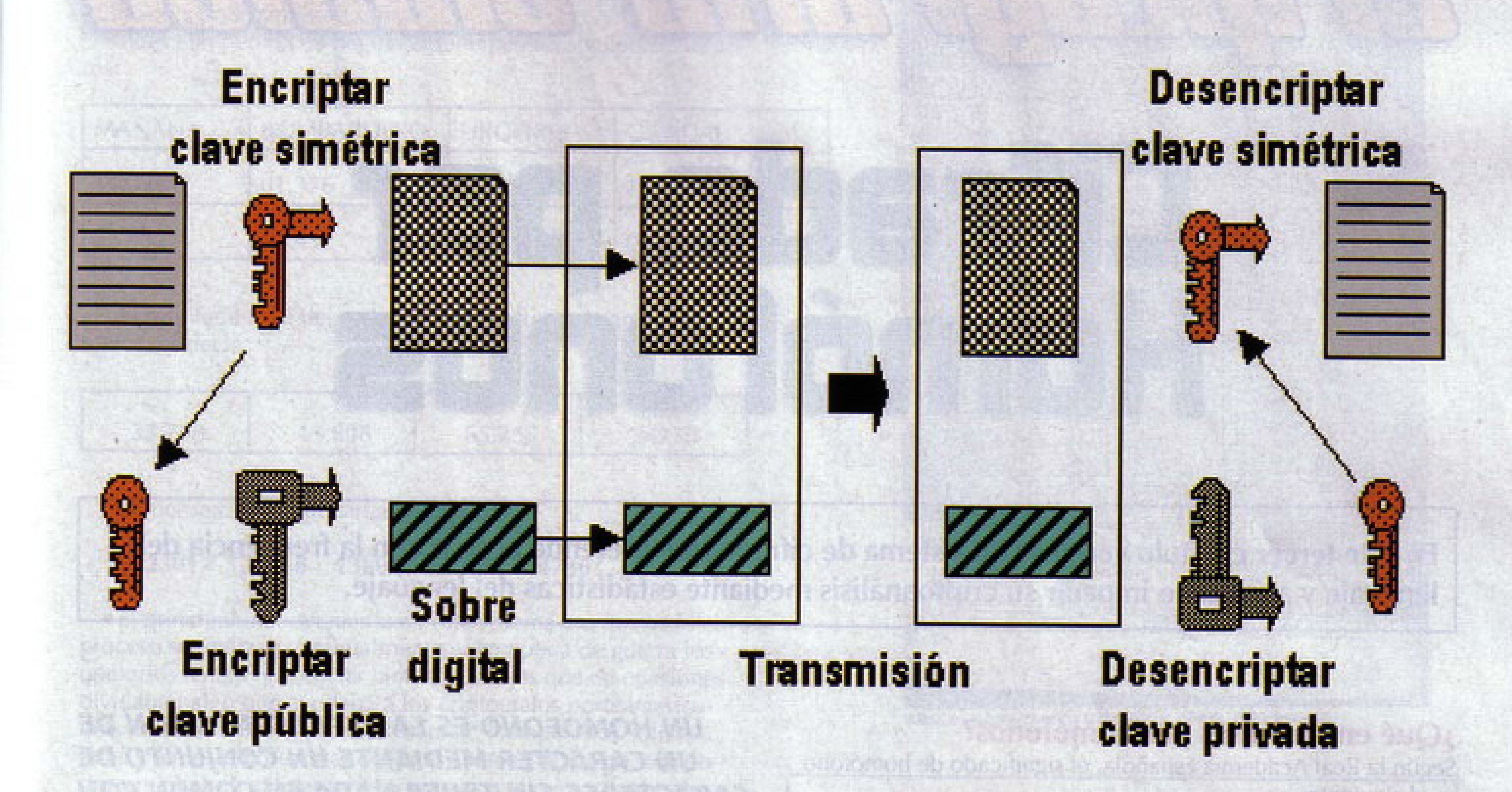
También el algoritmo DSA (por Digital Signature Algorithm, algoritmo de firma digital) del Departamento de Comercio de los Estados Unidos, y el PGP (por Pretty Good Privacy, privacidad bastante buena, en inglés), creado en 1991 por Philip Zimmermann y usado ampliamente para email, archivos, hasta particiones de discos enteras.

Seguridad de la firma digital

La firma digital proporciona un amplio abanico de servicios de seguridad, entre ellos están:

- **Autenticación:** permite identificar unívocamente al signatario, al verificar la identidad del firmante, bien como signatario de documentos en transacciones telemáticas, para garantizar el acceso a servicios distribuidos en red.
- **Imposibilidad de suplantación:** el hecho de que la firma haya sido creada por el signatario mediante medios que mantiene bajo su propio control (su clave privada protegida, por ejemplo, por una contraseña, una tarjeta inteligente, etc.) asegura, además, la imposibilidad de su suplantación por otro individuo, ya que no posee esa pieza inicial, por la que se creo la clave privada.
- **Integridad:** permite que sea detectada cualquier modificación por pequeña que sea de los datos firmados, proporcionando así una garantía ante alteraciones fortuitas o deliberadas durante el transporte, almacenamiento o manipulación telemática del documento o datos firmados.
- **No repudio:** esta característica ofrece seguridad de que el autor del documento no puede retractarse en el futuro de las opiniones o acciones consignadas en él ni de haberlo enviado. La firma digital adjunta a los datos un timestamp, debido a la imposibilidad de ser falsificada, testimonia que él, y solamente él, pudo haberlo firmado.
- **Auditabilidad:** permite identificar y rastrear las operaciones llevadas a ca-





bo por el usuario dentro de un sistema informático cuyo acceso se realiza mediante la presentación de certificados,

• El acuerdo de claves secretas: garantiza la confidencialidad de la información intercambiada ente las partes, esté firmada o no, como por ejemplo en las transacciones seguras realizadas a través de SSL (Secure Socket Layer).

Infraestructura Básica de la firma digital (PKI)

Esta clase de Infraestructura es también conocida como de "clave pública" o por su equivalente en inglés (Public Key Infrastructure, PKI).

La normativa crea el marco regulatorio para el empleo de la Firma Digital en la instrumentación de los actos internos del Sector Público Nacional que no produzcan efectos jurídicos individuales en forma directa, otorgándole a esta nueva tecnología similares efectos que a la firma hológrafa.

La disposición establece la configuración de la siguiente estructura:

· Organismo Licenciante (OL)
· Organismo Auditante (OA)
· Autoridad Certificada Licenciada (ACL)
· Suscriptores

Para comprobar la identidad del firmante y la integridad del mensaje, el receptor deberá generar la huella digital del mensaje recibido, luego desencriptará la firma digital del mensaje utilizando la clave pública del firmante y obtendrá de esa forma la huella digital del mensaje original; si ambas huellas digitales coinciden, significa que el mensaje no fue alterado y que el firmante es quien dice serlo.

LA CRIPTOGRAFÍA ASIMÉTRICA PUEDE SER APLICADA A NUMEROSOS MÉTODOS SIMÉTRICOS, YA QUE PERMITE SER UNA "CORAZA", QUE FACILITA LA DISTRIBUCIÓN DE CLAVES

Como sabemos, la clave privada de la persona, está alojada en la PC o registrada en una tarjeta inteligente, e identifica que un mensaje ha sido enviado por la persona. La segunda es una clave pública, que puede ser empleada por cualquiera que desee autenticar documentos que la persona firme. La clave pública 'lee' la firma digital creada por la clave privada de la persona y verifica la autenticidad de los documentos creados con la misma.

La clave privada de la persona se desbloquea mediante una contraseña o por tecnologías biométricas, como la retina, una huella digital o un rostro asociado con un registro de identidad.

Conclusión

La firma digital y los medios que implementan la criptografía asimétrica están ayudando muchísimo a las transacciones, y al mundo real, a relacionarlo con el mundo digital. A establecer esa relación tan dificultosa de identidad, integridad, veracidad. Quiero terminar diciendo que la criptografía asimétrica puede ser aplicada a numerosos métodos simétricos, ya que permite ser una "coraza", que facilita la distribución de claves.

Espero que les haya gustado tanto como a mí.

Nos vemos en la próxima.

SparK

http://www.disidents.org
http://www.intrabytes.com
spark@disidents.org
arielrm@intrabytes.com

criptografía clásica

Cifrado por Homófonos

En este tercer capítulo veremos un sistema de cifrado que pretende acabar con la frecuencia del lenguaje y así mismo impedir su criptoanálisis mediante estadísticas del lenguaje.

¿Qué entendemos por homófonos?

Según la Real Academia Española, el significado de homófono es el siguiente:

"Dicho de una palabra: Que suena de igual modo que otra, pero que difiere en el significado; p. ej., tubo y tuvo, huno y uno."

En criptografía un homófono es la representación de un carácter mediante un conjunto de caracteres sin tener nada en común con el carácter representado.

Por ejemplo, el carácter A podría representarse con los dígitos 82, los caracteres @R o algún sistema similar.

UN HOMÓFONO ES LA REPRESENTACIÓN DE UN CARÁCTER MEDIANTE UN CONJUNTO DE CARACTERES SIN TENER NADA EN COMÚN CON EL CARÁCTER REPRESENTADO

Nociones básicas sobre este sistema

Como dijimos al principio, mediante este sistema se puede evitar el criptoanálisis mediante estadísticas del lenguaje, esto es posible ya que a los caracteres de mayor frecuencia se le pueden asignar varios homófonos y transmitir un mensaje utilizando todos estos homófonos de forma equitativa, ya que si siempre se utilizan los mismos podría provocar que las frecuencias queden de nuevo repartidas en función al lenguaje y permitir un criptoanálisis mediante estadística.

Una sencilla forma de utilizar este sistema es asignando una numeración entre el 00 y 99 a los caracteres en función a su frecuencia, es decir, si el carácter E posee un 13% se le asignarán 13 homófonos diferentes, al carácter A con 10%, 10 homófonos y así con todos los caracteres del alfabeto. A la hora de transmitir un mensaje se utilizarán los 13 homófonos de la E de forma que se usen todos y queden repartidos a fin de que todos los homófonos del mensaje posean frecuencias similares y sea imposible un criptoanálisis mediante estadística.

A la hora de descifrarlo la tarea resulta sencilla, pues solo bastaría con recurrir al diccionario de homófonos, buscar el deseado y obtendríamos el texto en claro.

Un poco de historia

La utilización quizás más importante y reciente de este sistema quizás sea en el código JN-25 japonés o Japanese Navy 25, como lo llamaron los criptógrafos estadounidenses.

Este sistema se empleó por la fuerza naval japonesa durante la 2° Guerra Mundial. Se trataba de un sistema mejorado del cifrado por homófonos, ya que empleaba un diccionario, pero además una tabla de sumatorios.

El diccionario consistía en un conjunto de exactamente 33.333 letras, palabras y frases completas, es decir, una palabra o una frase completa podría quedar codificada en 5 dígitos entre 00000 y 99999, o simplemente uno de estos dígitos codificaba un solo carácter, lo que hacía de este sistema sumamente complicado de resolver.

Además de esto el sistema disponía de una seria de libros con tablas de sumarios. Cada libro disponía de 100 páginas, cada una de ellas con 15 líneas y 12 columnas, lo que hacía un total de 18.000 números.

Para cifrar un mensaje se procedía del siguiente modo:

Se buscaba en el diccionario la palabra en cuestión. En el diccionario aparecen por ejemplo los siguientes homófonos:

MAÑANA	BOMBARDERO	URGENTE	GUADALCANAL
11.326	01.376	21.843	14.863

Ahora se recurría a la tabla de sumatorios, se escogía una página, un número de columna y un número de fila, y a partir de ahí se continuaba columna abajo y después hacia la siguiente fila.



Si por ejemplo se escogía la página 072, la columna 30 y la fila 17 habría que comenzar el mensaje por la siguiente cifra: 0723017, de este modo en la recepción sabrían que hoja se ha utilizado y podrían descifrarlo.

Pues bien, en dicha página obtenemos los siguientes números:

MAÑANA	BOMBARDERO	URGENTE	GUADALCANAL
11.326	01.376	21.843	14.863
22.432	12.432	43.412	09.867

El resultado final del mensaje seria la suma de ambos números, es decir:

33.758	13.808	65.255	24730

El mensaje final quedaría:

0723017 33758 13808 65255 24730

El principal inconveniente de este sistema era que todo el proceso se realizaba manualmente, y en época de guerra los operarios tenían que enviar tantos mensajes que en ocasiones olvidaban algo que ayudaba a los criptógrafos norteamericanos, incluso, al ser el proceso manual, los operarios solían tener por costumbre cifrar con una cuantas tablas de sumatorios en lugar de utilizar todas y gracias a ello los criptógrafos podían saber quien había enviado el mensaje y tener una idea sobre el contenido del mensaje. Gracias a eso pudieron descifrar el código e incluso se cree que el ataque a Pearl Harbor se sabía con antelación pero hicieron como si no se supiese nada para que los japoneses no sospechasen que su código había sido descifrado.

Cifradores homofónicos de segundo orden

Este tipo de cifrado consiste en asignar homófonos en una cuadricula de Z x Z de tal modo, que un mismo mensaje pueda enviarse de dos formas diferentes si se cifra por columnas o por filas. Además este mismo sistema permite enviar dos mensajes diferentes, uno por filas y otro por columnas de tal modo que se puede enviar un mensaje falso y otro verdadero.

Con este tipo de cifrado se pretende crear un grado de incertidumbre sobre la veracidad de los mensajes, de este modo, aunque se logre descifrar el mensaje no se sabrá cuál de ellos es el verdadero, y esto en algunos casos puede ser muy ventajoso para quien lo envía, ya que el enemigo posiblemente no tendrá tiempo cual de los mensajes es el verdadero.

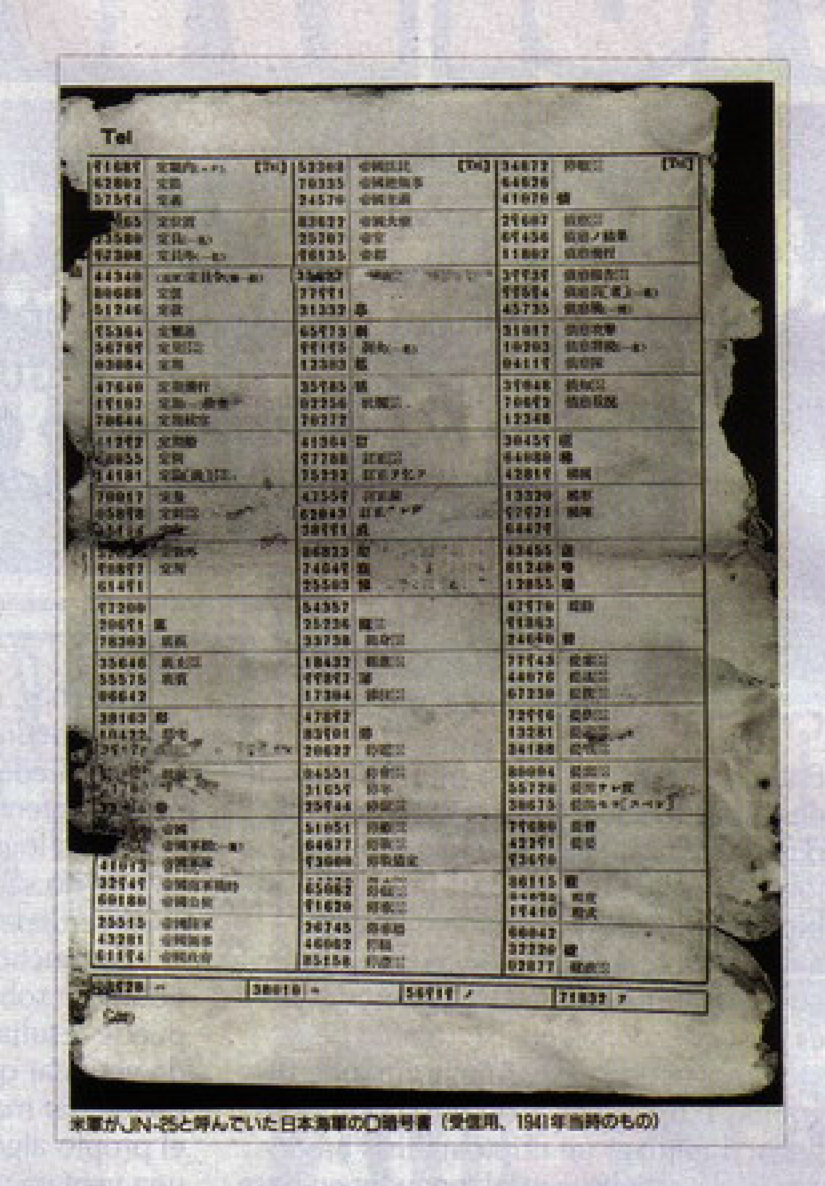
Además, con este sistema se consigue que cada carácter posea un total de Z homófonos tanto para las columnas como para las filas.

Para enviar un mensaje, tan solo necesitaríamos dos frases o palabras con el mismo número de caracteres y coger el homófono común a carácter M1(i) y M2(i), de tal modo que puedan leerse los dos por columnas o por filas.

Si tenemos la tabla de homófonos (Tabla 1), podríamos enviar los siguientes dos mensajes del siguiente modo:

M1: ATAQUE INMINENTE GUADALCANAL
M2: ORDENA RENDICION TOTAL MAÑANA

Ambos mensajes poseen 26 caracteres, pero el contenido



米軍がJN-25と呼んでいた日本海軍の暗号書（受信用、1941年当時のもの）

de ambos en bien distinto.

Para cifrar el primer carácter de ambos mensajes, A y O, tendríamos que buscar el homófono común a ellos dos, siendo A columnas y O filas. Dicho homófono seria: 406

Visto esto, el mensaje final quedaría:

406 507 82 126 373 5 495 122 364 90 230 59 230 426 356 547 427 541 4 298 336 3 379 14 352 363

Criptoanálisis

Este tipo de sistemas son muy difíciles de descifrar debido a que, a diferencia de otros sistemas, la asignación de homófonos no sigue una lógica sino que más bien se asignan de forma arbitraria. La mejor forma, y para ello hay que contar con una gran cantidad de texto cifrado, es buscar cadenas que se repitan constantemente en el mensaje, formando digramas o trigramas. Con esto podríamos llegar a realizar un criptoanálisis basándonos en estadística del lenguaje en base a esos digramas o trigramas, aunque ello suele resultar igualmente complicado de descifrar.

LA ASIGNACIÓN DE HOMÓFONOS NO SIGUE UNA LÓGICA SINO QUE MÁS BIEN SE ASIGNAN DE FORMA ARBITRARIA

Además, si topamos con un mensaje cifrado mediante un sistema de segundo orden, puede que después de mucho tiempo intentando descifrarlo, cuando por fin lo logremos no obtengamos nada ya que no sabremos cual de los mensajes es el verdadero.

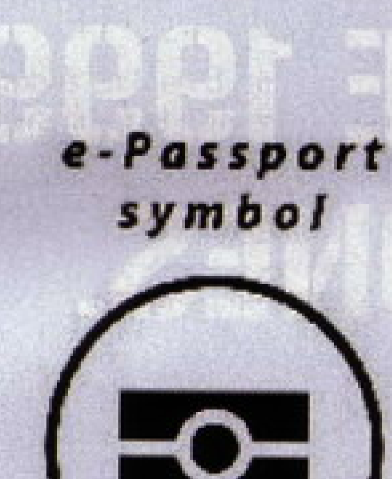
En muchos casos, este grado de incertidumbre sobre la veracidad del mensaje puede resultar incluso más complicado de verificar que el propio sistema y esto puede dar más seguridad al sistema que el propio algoritmo de cifrado, lo cual es una ventaja para quien envía el mensaje.

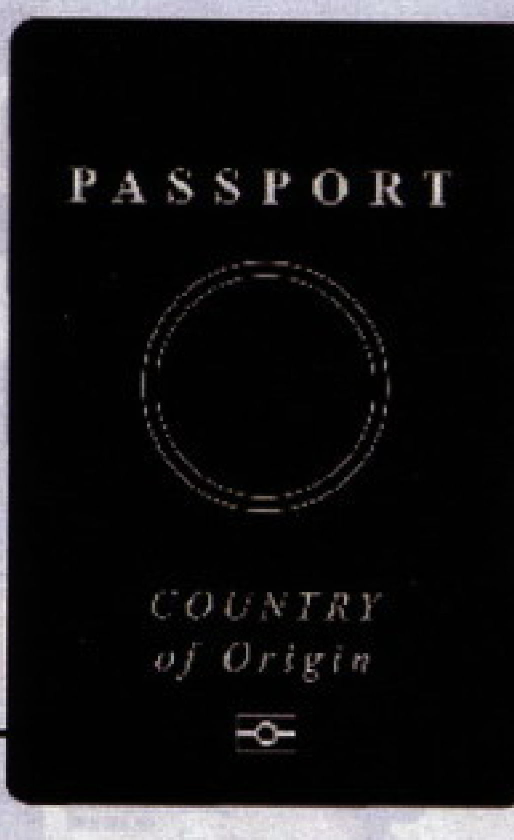
TheBlooD

(暗號ノ三)

072

	91	50	24	73	56	39	02	15	44	81	54	70
16	14929	35628	80562	00147	88137	93504	21500	58665	97820	17326	56853	01076
85	23183	63451	07541	65326	38003	42353	94004	78478	04047	33017	30748	52211
32	36831	78346	33669	43223	01494	14713	40230	32562	58607	01712	08545	94076
17	31819	48704	11557	81078	90567	25006	84061	67611	40964	47620	97947	17795
98	61324	58431	06434	33724	57532	75084	54976	16316	30250	52377	49357	66013
05	44635	05883	21137	67209	29321	98312	05937	89563	74078	00156	87874	24512
33	53252	04722	58423	82158	76830	49301	39100	77283	20120	72090	15782	03640
95	97453	22039	61220	56431	41787	34328	78163	16194	85460	25594	78566	25939
07	81563	70850	41526	18789	60024	54267	10645	09150	62621	65227	16312	93190
52	02843	83298	74802	03172	15640	26854	02163	92218	13056	84914	64117	11285
46	85513	62153	95276	31374	04282	80618	63245	36922	80083	45706	08807	71053
11	90452	41881	52291	99360	70718	61941	88117	12267	73010	10542	88902	40263
04	13767	23648	72923	48762	52650	12805	49350	28594	07034	37760	20865	56021
72	27364	30467	87101	28450	32180	68543	03360	58470	69311	98487	38180	89513
69	09317	52563	19755	76921	24866	45705	27023	03800	22084	59410	76035	04010

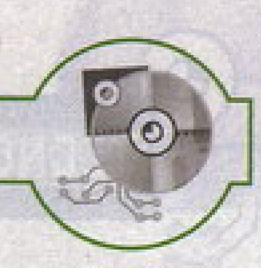


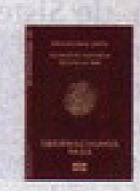




Pasaportes electrónicos: mecanismos de seguridad avanzada

En el capítulo anterior introducimos al lector en los mecanismos de seguridad de los nuevos pasaportes electrónicos. Explicamos detalladamente los mecanismos de autenticación pasiva y activa. Sin embargo, estas medidas de seguridad pueden no ser suficientes. Por este motivo han sido propuestos nuevos mecanismo de seguridad como veremos a continuación.







Par de claves estáticas:

$$(SK_{PICC}, PK_{PICC}, \mathcal{D}_{PICC})$$

Selecciona aleatoriamente un par de claves efímeras:

$$\xrightarrow[\mathcal{D}_{PICC}]{PK_{PICC}}$$

$$(\widetilde{SK_{PCD}}, \widetilde{PK_{PCD}}, \mathcal{D}_{PICC})$$

$$\xleftarrow{\widetilde{PK_{PCD}}}$$

$$K = \mathbf{KA}(SK_{PICC}, \widetilde{PK_{PCD}}, \mathcal{D}_{PICC}) \qquad K = \mathbf{KA}(\widetilde{SK_{PCD}}, PK_{PICC}, \mathcal{D}_{PICC})$$

Autenticacion del chip.

Control de Acceso

Los mecanismos de control de acceso utilizados en los pasaportes electrónicos son necesarios tanto para garantizar la privacidad de sus usuarios como para disminuir las amenazas de clonación de los mismos. El chip incorporado en los pasaportes protege el acceso a los datos almacenados mediante los siguientes mecanismos de control de acceso:

- **Datos poco sensibles.** Se consideran datos poco sensibles aquellos que se puedan adquirir fácilmente por otras fuentes (ej. imagen facial). Esta tipo de información es controlada por el control de acceso básico.
- **Datos altamente sensibles.** Se consideran datos altamente sensibles aquellos que no pueden obtenerse a gran escala por otras fuentes (ej. huellas digitales). Tales datos son protegidos mediante el control de acceso extendido.

Control de Acceso básico

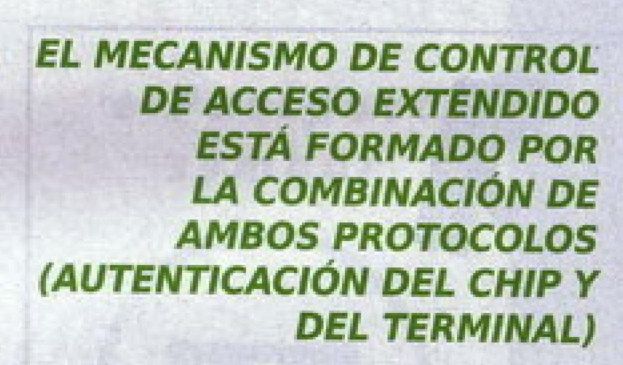
Aunque ya explicamos este mecanismo en el artículo anterior recordaremos al lector sus aspectos más relevantes. El lector debe demostrar al chip incorporado en el pasaporte que conoce la información impresa en el pasaporte en la zona del código de lectura automática (MRZ) antes de que este transmita alguna información. El lector le enviará una solicitud al chip, el cual le devolverá un reto. El lector firmará el reto y se lo devolverá al chip junto con un mensaje de autenticación. Mediante la información leída en la zona del MRZ, se obtiene una semilla que se utilizará para la generación de las claves utilizadas en la firma y en el mensaje de autenticación. En el mensaje firmado por el lector se incluye un nuevo reto. Si el lector es autenticado correctamente el chip enviará un mensaje firmado de este nuevo reto junto con un mensaje de autenticación de forma similar a como hizo el lector. El lector comprobará la validez de los mismos y si son correctos el lector y el chip (pasaporte) estarán autenticados mutuamente. Una vez establecida la autenticación mutua, se establecerá una clave de sesión que será utilizada para garantizar la confidencialidad e integridad de las comunicaciones.

Mecanismos de seguridad avanzada

Se definen dos mecanismos de seguridad avanzada para los pasaportes electrónicos: autenticación del chip y autenticación del terminal (lector).

La autenticación del chip puede ser utilizada como una alternativa al mecanismo opcional de autenticación

EL LECTOR DEBE DEMOSTRAR AL CHIP INCORPORADO EN EL PASAPORTE QUE CONOCE LA INFORMACIÓN IMPRESA EN EL PASAPORTE EN LA ZONA DEL CÓDIGO DE LECTURA AUTOMÁTICA (MRZ) ANTES DE QUE ESTE TRANSMITA ALGUNA INFORMACIÓN



EL MECANISMO DE CONTROL DE ACCESO EXTENDIDO ESTÁ FORMADO POR LA COMBINACIÓN DE AMBOS PROTOCOLOS (AUTENTICACIÓN DEL CHIP Y DEL TERMINAL)

activa. Ambos protocolos permiten la verificación de la autenticidad del chip. Sin embargo, la autenticación activa ofrece algunas ventajas: establecimiento de una clave de sesión garantizado la seguridad de las comunicaciones así como un mayor nivel de seguridad.

La autenticación del terminal permite verificar al chip que el sistema de inspección (lector) tiene derechos de acceso a la información almacenada en el mismo. Debido a que el sistema de inspección puede acceder a información altamente sensible, las comunicaciones deben estar protegidas apropiadamente. Por este motivo, previo a la autenticación del terminal, el mecanismo de autenticación del chip debe haber sido ejecutado satisfactoriamente. El mecanismo de control de acceso extendido está formado por la combinación de ambos protocolos (autenticación del chip y del terminal).

Procedimiento de inspección

Podemos clasificar los dispositivos atendiendo a su conformidad o no conformidad con la especificación. Los dispositivos se clasificarán como sistemas de inspección estándar y sistemas de inspección avanzada.

Los sistemas de inspección estándar se utilizarán siempre que la información almacenada en los mismos no sea altamente sensible.

Los sistemas de inspección avanzada se utilizará siempre que esté en juego información altamente sensible.

Infraestructura de clave pública

La autenticación del terminal requiere que el sistema de inspección pruebe al chip incorporado en el pasaporte que éste tiene derechos de acceso a la información sensible almacenada en el mismo. El sistema de inspección estará equipado con, al menos un, "Certificado de Sistema de Inspección". Este certificado contendrá la clave pública del sistema de inspección y sus derechos de acceso. Asociada a esta clave pública, el sistema de inspección poseerá su clave privada. Una vez que el sistema de inspección haya demostrado el conocimiento de esta clave privada, el chip del pasaporte le dará acceso al mismo de acuerdo con los derechos de acceso especificados en el certificado.

La infraestructura de clave pública consistirá en las siguientes entidades: autoridades de verificación estatal (CVCAs), autoridades de verificación de documentos (DVs) y sistemas de inspección (ISs).

Sistema de Inspección	Chip Pasaporte electrónico	
	Conformidad	Disconformidad
Conformidad	Avanzada	Estándar
No conformidad	Estándar	Estándar

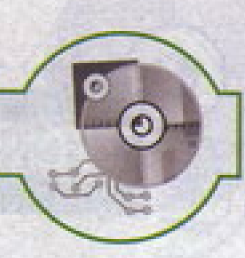
Autoridad de verificación estatal (CVCAs)

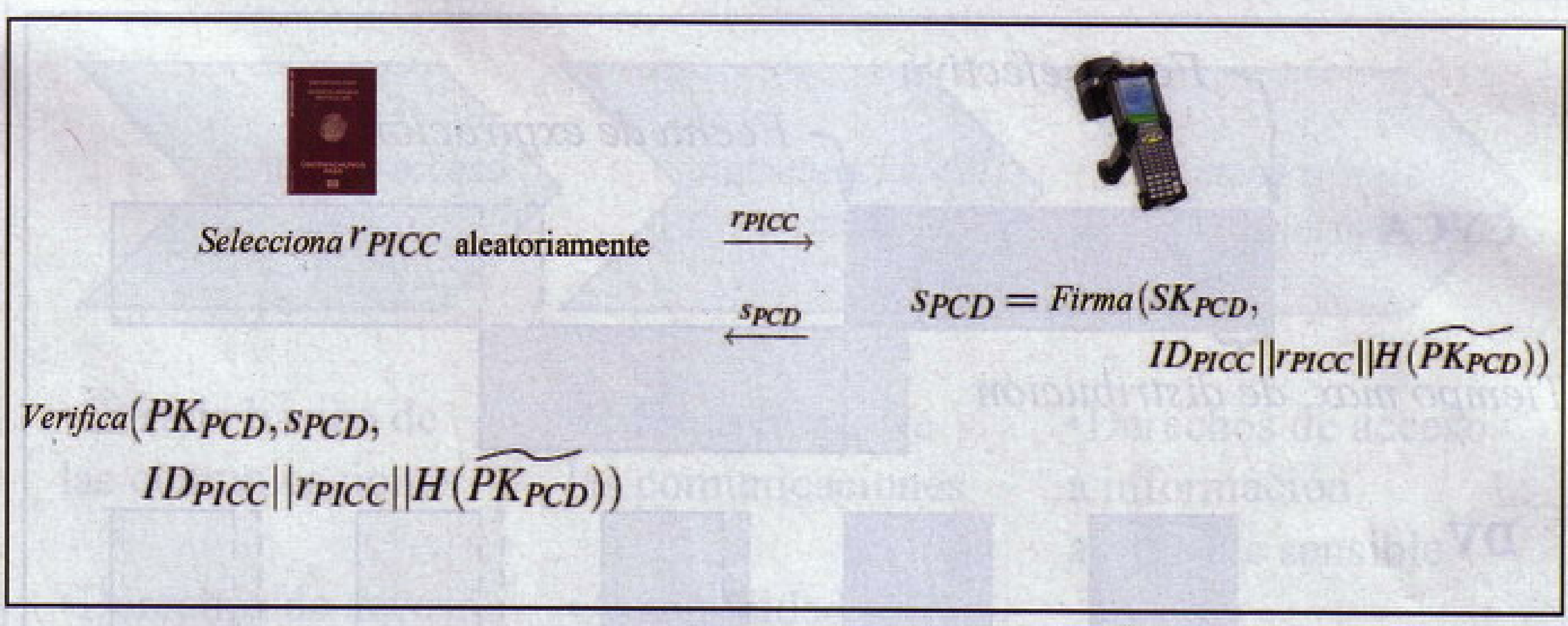
Cada estado debe tener una autoridad de certificación encargada de las autoridades de verificación de los documentos. El CVCA determina los derechos de acceso a los pasaportes electrónicos para todas las autoridades de verificación de documentos. Concretamente, el CVCA emitirá un certificado a cada una de estas entidades, en el cual se especificará la información a la que tienen acceso. Con el objetivo de mitigar los potenciales riesgos que traería asociados el robo de un certificado de este tipo, el periodo de validez del mismo debería no ser muy largo.

Autoridad de verificación de documentos (DVs)

Es una entidad encargada de un conjunto de sistemas de verificación para los cuales emitirá un certificado. Por tanto una autoridad de verificación de documentos es una autoridad de certificación, autorizada por, al menos la autoridad de verificación nacional (CVCA), para la emisión de certificados para los sistemas de inspección nacionales. Normalmente, tanto los derechos de acceso como el periodo de validez de los certificados emitidos por el DV, son idénticos a los de esta entidad. Sin embargo, el DV podría imponer restricciones.

Si un sistema de verificación requiere que sus sistemas de inspección puedan tener acceso a información sensible almacenada en pasaportes de otros países., este tendrá que solicitar





Autenticacion del terminal.

un certificado de autoridad de verificación de documentos a la autoridad de verificación estatal de dicho país.

Sistemas de inspección (ISs)

El nivel más bajo de la infraestructura de clave pública, son los lectores de los pasaportes electrónicos, también conocidos como sistemas de inspección, los cuales permiten el acceso a la información sensible.

Periodo de validez

Como hemos comentado anteriormente, uno de los puntos débiles asociado a la utilización de certificados es el robo de los mismos. Para mitigar los posibles riesgos de seguridad, el periodo de validez de los mismos no debería ser demasiado largo. Todo certificado debe tener un periodo de validez el cual es identificado por dos fechas. Primero tenemos el "día efectivo del certificado", que es la fecha cuando fue emitido el certificado. En segundo lugar tenemos el "día de expiración del certificado" que es la fecha a partir de la cual el certificado deja de ser valido.

La renovación de los certificados debe planearse con antelación, siempre teniendo en cuenta el tiempo de distribución del certificado. Obviamente, el certificado no puede emitirse antes que el certificado actual expire. El tiempo máximo de distribución debe ser igual a la diferencia ente el día de expiración y el día efectivo del nuevo certificado.

Validación de un certificado

Uno de los puntos clave de los mecanismos de control de acceso avanzado es la verificación de un certificado. Para validar un certificado de la autoridad de inspección, se debe proporcionar una "cadena de certificado" al chip incorporado en el pasaporte, comenzando en el punto de confianza almacenado en el mismo. Estos puntos de confianza serán las claves públicas de las autoridades de verificación estatal. El punto de acceso inicial será almacenado en el periodo de producción o en la fase de personalización en el chip.

El chip sólo aceptará certificados recientes del sistema de inspección. Si el chip no tiene reloj interno, la fecha actual será aproximada de la forma siguiente: el día actual almacenado en el chip es inicialmente el día de personalización del mismo. Este día será automáticamente aproximado en el chip usando el certificado válido más reciente de la autoridad de certificación estatal, la autoridad de certificación de documentos o el sistema de inspección. El sistema de inspección puede mandar alguno de estos certificados al chip a fin de actualizar tanto la fecha actual como sus puntos de confianza, independientemente de si el proceso de autenticación con el terminal va a continuar.

La validación de un certificado la podemos dividir en dos fases:

TODO CERTIFICADO DEBE TENER UN PERIODO DE VALIDEZ EL CUAL ES IDENTIFICADO POR DOS FECHAS



Fecha efectiva

Fecha de expiración

CVCA

Tiempo max. de distribución

DV

IS

Planificación de certificados.

Verificación del certificado. La firma debe ser validada y el certificado no debe haber expirado. Si alguna de estas dos condiciones no se mantienen el proceso es abortado.

Actualización del estado interno: La fecha actual debe ser actualizada, y las claves públicas y atributos deben ser importadas. A su vez nuevos puntos de confianza deben ser añadidos y aquellos que hayan expirados será eliminados.

Ejemplo de Autenticación del Terminal

La autenticación del terminal la podemos dividir en cuatro pasos:

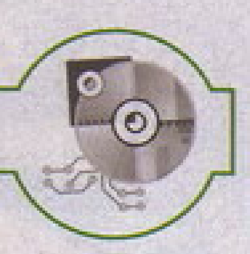
El sistema de inspección envía una "cadena de certificado" al chip del pasaporte. La cadena comienza con un certificado verificable con la clave pública de la autoridad de verificación estatal y termina con el certificado del sistema de inspección.

Para cada certificado recibido, el chip realizará los siguientes pasos:

El chip verificará la firma del certificado. Si la firma es incorrecta, la verificación será fallida.

La fecha de expiración del certificado es comparada con la fecha actual del chip. Si la fecha de expiración es anterior a la fecha actual, la verificación será fallida.

El certificado es validado y la clave pública y los atributos más relevantes contenidos en el certificado son importados. Para los certificados de verificación estatal la clave pública es añadida a la lista de puntos de confianza almacenados en una zona de memoria segura en el chip. A partir de este momento, el nuevo punto de



Control de acceso básico	Autenticación del chip	Autenticación del terminal
•Cifrado básico de las comunicaciones	•Cifrado fuerte de las comunicaciones	•Derechos de acceso a información altamente sensible
•Derechos de acceso a datos sensibles	•Autenticidad del chip	•Lectura de datos altamente sensibles (huellas digitales)
•Lectura de la clave pública del chip	•Lectura de datos sensibles (imagen facial)	

Mecanismos de Autenticació n.

L A VALIDACIÓN DE UN CERTIFICADO LA PODEMOS DIVIDIR EN DOS FASES: VERIFICACIÓN DEL CERTIFICADO Y ACTUALIZACIÓN DEL ESTADO INTERNO

confianza está disponible. Para los certificados de verificación de documentos y sistemas de inspección la clave pública se importa temporalmente para las subsecuentes verificaciones de certificados o la autenticación del terminal, respectivamente.

La fecha efectiva de los certificados se compara con la fecha actual del chip. Si la fecha actual es anterior a la fecha efectiva, la fecha actual del chip es actualizada a la fecha efectiva del certificado.

Llegados a este punto el chip enviará un reto (rPICC) al sistema de inspección.

El sistema de inspección responderá con la firma del reto, para lo cual empleará su clave privada (SKPCD):

```
SPCD=
Sign(SKPCD,IDPICC||r
PICC||H(PKPCD))
```

Siendo PKPCD la clave pública del sistema de inspección e IDPICC el número de documento del pasaporte incluyendo los dígitos de control (similar al control de acceso básico).

El chip verificará la firma con la clave pública del chip (PKPDC):

```
Verificar (PKPDC, SPDC,
IDPICC||rPICC||H(PKPCD))
```

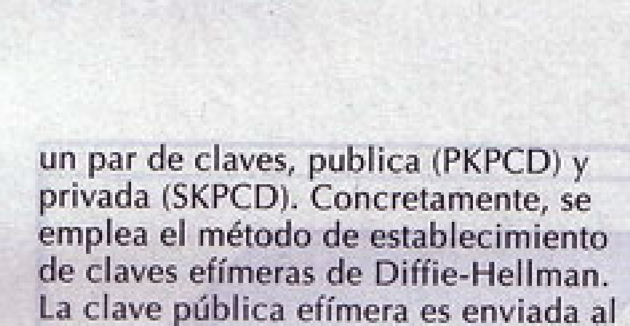
Todos los mensajes deberán ser transmitidos de forma segura (cifrado), a través de la clave de sesión establecida en el mecanismo de autenticación del chip.

Ejemplo de autenticación del chip

La autenticación del terminal la podemos dividir en tres pasos:

El chip del pasaporte enviará al sistema de inspección su clave pública (PKPICC) así como sus parámetros de dominio (DPICC). Esta clave pública tendrá asociada una clave privada (SK-PICC), la cual se almacenará de forma segura en el pasaporte.

El sistema de inspección generará



un par de claves, publica (PKPCD) y privada (SKPCD). Concretamente, se emplea el método de establecimiento de claves efímeras de Diffie-Hellman. La clave pública efímera es enviada al chip.

Ambos, el sistema de inspección y el chip del pasaporte realizan los siguientes cálculos:

Establecen una clave compartida entre ambos: K = KA(SKPICC, PKPCD, DPICC) = KB(SKPDC, PKPICC, DPICC).

A partir de K se deriva una clave de sesión.

Para verificar la autenticidad de la clave pública del chip, el sistema de inspección deberá iniciar el proceso de autenticación pasiva inmediatamente después de la autenticación del chip.

Enlaces

Extended Access Control: http://www.bsi.de/fachthem/epass/eac.htm
Pasaporte electrónico en España: http://www.safelayer.com/content/view/107/84/
Internacional Civil Aviation: http:// www.icao.int/
Machine Readable Travel Documents: http://mrtd.icao.int/

Conclusiones

En la actualidad estamos en la primera fase de implantación de los pasaportes electrónicos. Como vimos en el anterior artículo, la seguridad de los mismos podría no ser la suficiente. En la segunda fase de implantación de estos dispositivos se prevé la incorporación de información altamente sensible como puede ser las huellas digitales (2010). Por tanto, no cabe duda de que son necesarias nuevas medidas de seguridad. Concretamente, ha sido propuesto el mecanismo de control de acceso extendido. La seguridad de este mecanismo reside en la criptografía de clave pública por lo que es necesaria la implementación de una infraestructura de clave pública. En España Indra con el apoyo de Safelayer será los responsables de su implantación.

Pedro Peris López



soul ★ r&b ★ urban ★ funk ★ j
SOUL NATION
PRECIO 3'95€
NÚMERO 5 A LA VENTA EL 1 DE OCTUBRE
SN
PRINCE
MICHEL CAMILO
MACEO PARKER
BILLIE HOLIDAY
KENDRA ROSS
THE JAMES TAYLOR QUARTET
DONNY HATHAWAY
RAHSAAN PATTERSON
TOK TOK TOK
DOO WOP
KEITE YOUNG
CANDY DULFER
ALICIA KEYS
N'DEA DAVENPORT
DIARGI
TUOMO
LEDISI
KEYSHIA COLE
MARCUS JOHNSON
GUATEQUE ALL STARS
LOS FULANOS
OKE
WILL.I.AM
NUEVO RETO
WILL.I.AM · ALICIA KEYS · PRINCE · MICHEL CAMILO
MACEO PARKER · RAHSAAN PATTERSON · BILLIE HOLIDAY
THE JAMES TAYLOR QUARTET · DONNY HATHAWAY
GUATEQUE ALL STARS · N´DEA DAVENPORT · DOO WOP
KEITE YOUNG · CANDY DULFER · TOK TOK TOK · DIARGI
KENDRA ROSS · TUOMO · LEDISI · KEYSHIA COLE
MARCUS JOHNSON · LOS FULANOS · OKE ...
Además: Soul Movies, Classics, 10 Delicatessen, Soul Art, Conciertos, Discos...
Precio 3,95 €
www.soulnation.es
info@soulnation.es
www.myspace.com/soulnationmagazine



Resolver problemas de apagado de Windows

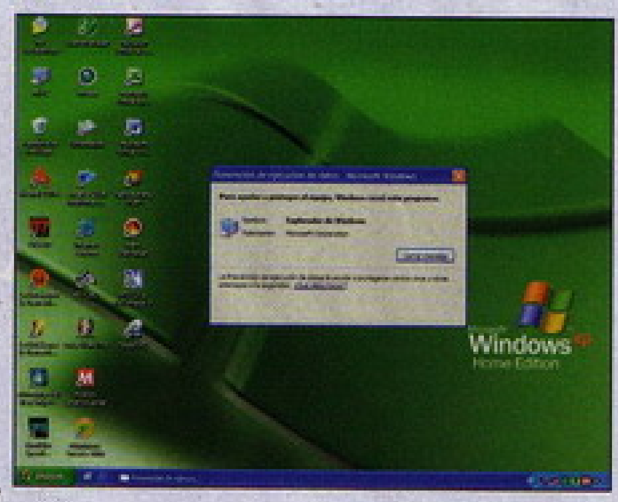
Pese a que a muchos nos preocupa inicialmente que el ordenador se inicie correctamente (¡qué menos!), lo cierto es que este acto tan básico - y a la vez tan complejo - puede tener mucho que ver con que previamente se haya cerrado adecuadamente el sistema, un proceso que no siempre es tan evidente como cabría esperar.

Windows XP ha conseguido, a lo largo de estos últimos años, hacerse con el liderato en el mundo de los sistemas operativos, siendo utilizado por millones de usuarios a lo largo y ancho del planeta. Muchos de estos (la gran mayoría seguramente) se habrá topado a lo largo de sus vidas con un problema muy común y que consiste en el que el sistema no se termina de apagar, es decir que al proceder con el método tradicional de apagado haciendo clic en el menú "Inicio - Apagar equipo", la máquina no se da por aludida, como si hubiera adquirido vida propia decidiendo que no eres quién para ordenarle cuando desconectarse o no.

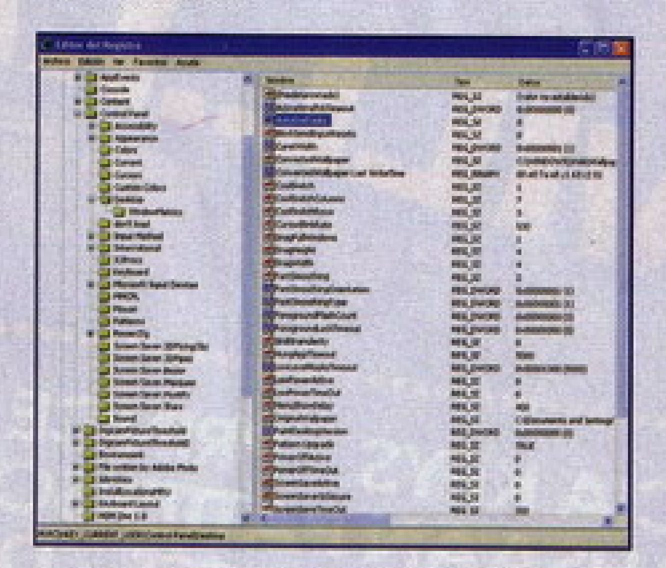
Lo que realmente está ocurriendo (a falta que la ciencia evolucione tanto como para que la inteligencia artificial de nuestro sistema adquiera un nivel de conciencia al estilo del ordenador HAL 9000 del clásico 2001 Odisea del Espacio de Kubrick) es que una o más aplicaciones están truncando el cierre debido a que alguna tarea o tareas se mantiene activa impidiendo que el ordenador pueda apagarse.

Algo aparentemente tan trivial puede acarrearnos consecuencias funestas si no procedemos con cierta cautela puesto que el acto (casi reflejo) al que todo hijo de vecino acabará llegando será el famoso "botonazo", la solución más radical a la vez que efectiva de poner fin a nuestra sesión, esto es, pulsar en el botón de encendido/apagado del PC y, en el caso que esto tampoco funcione como esperamos, pulsar este botón durante unos pocos segundos hasta que el sistema se apague definitivamente.

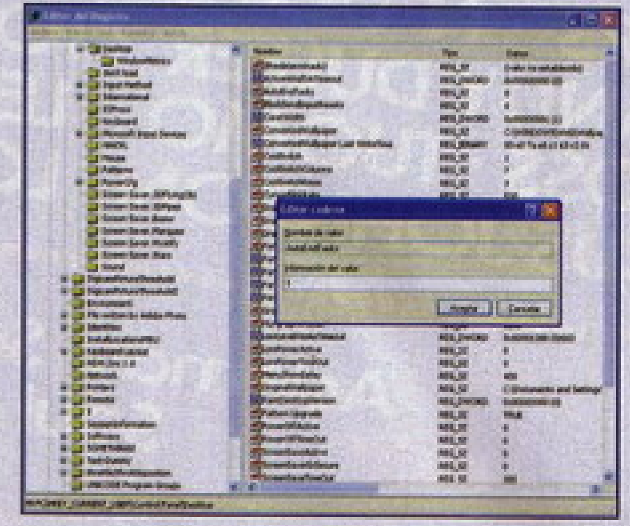
Podría pensarse que el objetivo principal se ha cumplido, no obstante lo cierto es que un cierre tan traumático del PC es habitualmente el responsable de que a la postre se desencadenen errores durante



1.- Error que puede aparecer durante el cierre de Windows.



2.- Los cierres pueden optimizarse desde el registro del sistema.



3.- Cambiando este valor permitiremos un cierre menos traumático.

el reinicio, aplicaciones que comienzan a funcionar caóticamente, cuando no directamente mal, archivos que observamos impotentes como irrecuperables, un ralentizamiento sustancial de la máquina y, en el peor de los casos, fallos durante el reinicio y hasta problemas de arranque de nuestro imprescindible sistema operativo.

En Windows XP sin embargo podremos resolver esta circunstancia de una manera bastante efectiva, de forma que el sistema se apague correctamente pese a que alguna aplicación trate de impedirlo, cerrándola de la forma menos problemática posible y preservando en todo lo posible la integridad de la máquina. Para ello será necesario que accedamos y editemos un parámetro en concreto dentro del registro de Windows haciendo uso del editor del mismo.

Par ello haremos clic en "Inicio - Ejecutar", escribimos "regedit" en la casilla (sin las comillas) y pulsamos en el botón Aceptar. Esto nos abre el tradicional editor que nos mostrará a la izquierda una estructura arbórea que podremos recorrer y a la derecha una serie de parámetros asociados a cada una de las ramificaciones existentes. Allí deberás buscar la siguiente ruta:

```
HKEY_CURRENT_USER \
Control Panel \ Desktop
```

Desde este punto es posible cambiar toda una serie de opciones del sistema pero la que nos interesa en esta ocasión es el parámetro llamado "AutoEndTasks". En nuestro caso deberemos cambiar el valor que trae por defecto. Con este objetivo debemos hacer doble clic sobre él lo que nos mostrará una nueva ventana que muestra el valor "0" que será necesario cambiar por el número "1". Esto tendrá como efecto inmediato la eliminación automática las tareas en el proceso de apagado del sistema. Aceptamos los cambios cerrando esta ventana y, a continuación el registro y, para confirmar los cambios, será conveniente reiniciar el sistema.

A partir de este instante Windows XP cerrará todas las aplicaciones, aunque no quieran hacerlo, cuando se solicite el apagado del equipo, sin que sea necesaria la intervención del usuario.

Nicolás Velásquez Espinel

Detectar problemas con el visor de sucesos

Nuestro PC puede ser víctima de un sinfín de situaciones que pongan en riesgo su funcionamiento por lo que una identificación correcta (y a tiempo) de los problemas puede llegar a ser vital cara a la supervivencia del sistema. De ahí que hacer un buen uso de herramientas como el visor de sucesos debe tenerse muy en cuenta.

Nuestro sistema supervisa los eventos del sistema y guarda un registro de todo lo que acontece, incluyendo errores y mensajes de aviso. Con el visor de sucesos, que viene ya "de serie" a partir de Windows XP/2000 es posible supervisar estos sucesos almacenados en el registro del mismo nombre. Y es que normalmente un equipo salvaguarda los registros de Aplicación, Seguridad y Sistema, aunque también puede contener información de otros registros, dependiendo de la función del equipo y de las aplicaciones instaladas.

Para poder ver tales datos será posible emplear el visor de Sucesos, una aplicación que forma parte de la consola de administración de Microsoft (Microsoft Management Console: MMC) de Windows, una consola que contiene herramientas administrativas para la gestión de redes, equipos, servicios y otros componentes. Con el fin de solucionar algún problema del sistema puedes abrir la consola Administración de equipos (para ello puedes hacer clic en Inicio, luego con el botón derecho del ratón sobre Mi PC y de ahí selecciona Administrar). Tras abrirlo haz doble clic en el visor de sucesos (bajo la rama Administración del equipo - Herramientas del sistema - visor de sucesos) y selecciona uno de los tres apartados: Sistema, Aplicaciones o Seguridad (sobre todo se usan los dos primeros).

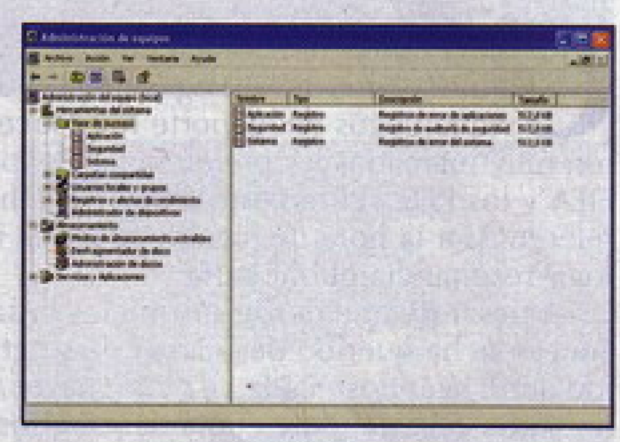
El registro más usado es el del Sistema, ya que recoge las incidencias de funcionamiento del sistema operativo. Cada vez que se arranca el sistema el módulo "Eventlog" añade un suceso al registro del sistema indicando que se ha activado el servicio de registro de sucesos. Si recorremos la lista de sucesos hacia arriba podremos comprobar si algún servicio o dispositivo no funciona correctamente. El caso más usual, es el mal funcionamiento del adaptador de red, suele generar una cascada de sucesos, dada la interdependencia de los servicios de red.

El registro de Seguridad almacena los sucesos generados por el sistema de auditoria (este se activa desde al administrador de usuarios) mientras que el registro de aplicaciones es el lugar donde las aplicaciones de usuario, tales como servidores de bases de datos y de información, registran sus sucesos, de manera que no interfieren con los generados por el sistema.

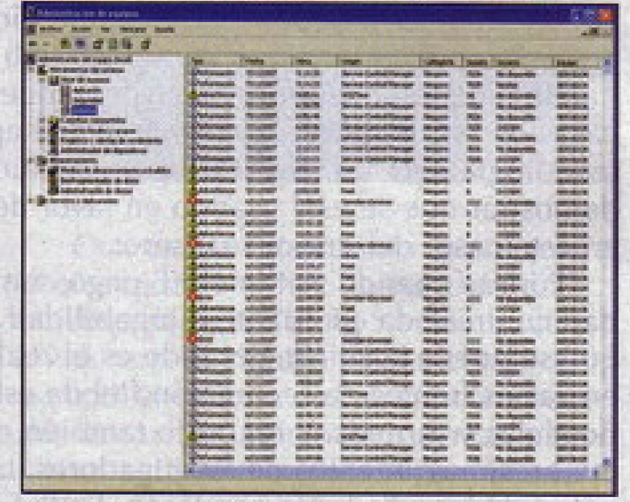
Cada apartado alberga 512 KB de información, lo cual suele bastar para varias semanas de datos. Para mantener únicamente los avisos y errores relativos a Sistemas y Aplicaciones, elige "Ver - Filtro" de la aplicación y desactiva la marca de Información. A continuación haz clic en Aceptar para examinar dichos registros.

Para lograr acceder a más detalles sobre un suceso, haz doble clic directamente sobre él. A continuación puedes pulsar el enlace que hay debajo de Descripción y pinchar en "Sí" para que el suceso sea enviado a Microsoft a través de Internet (cosa que te permitirá averiguar más datos sobre el problema y quizás solucionarlo de paso).

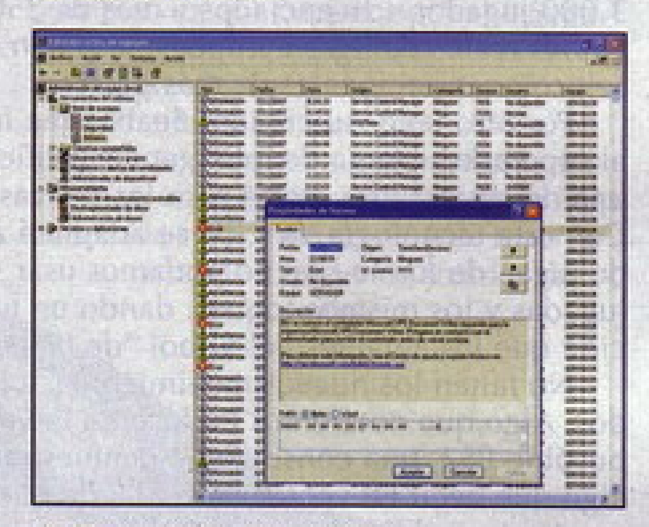
Si por ejemplo un controlador no funciona correctamente es posible que en el visor de sucesos puedas ver un icono de error al lado de una referencia a dicho controlador (bien sea de error o de advertencia). Si haces doble clic sobre el dispositivo que marca el error accederás a otra ventana en la que se muestra la causa del error. Allí podrás observar cómo cada línea del registro está formada por un icono, que indica la importancia del suceso, la fecha y hora en que se produjo el suceso, el módulo del sistema que ha



1.- La consola de administración de equipos da acceso al visor de sucesos.



2.- Lista de sucesos.

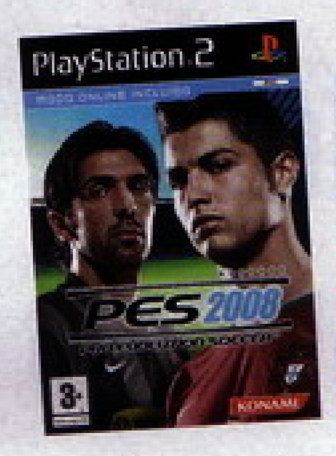


3.- Propiedades de sucesos.

generado el suceso, la categoría en la que se haya clasificada el suceso, el número de identificación del suceso, el usuario que ha generado el suceso y el ordenador en el que se ha generado el suceso.

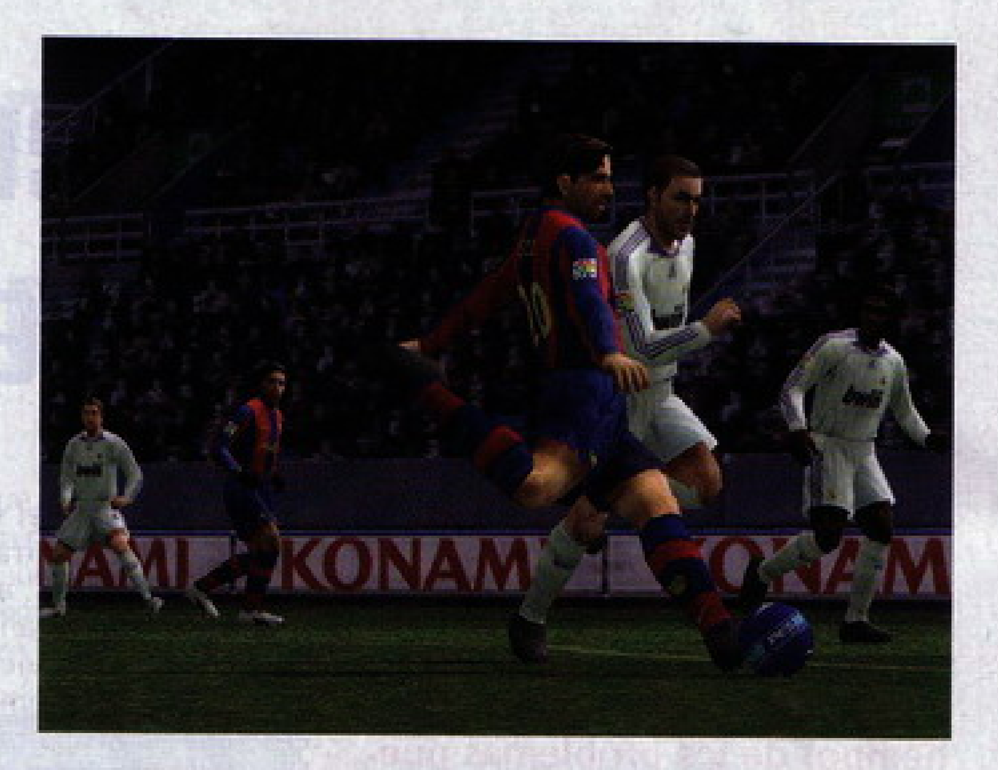
En definitiva toda una serie de datos informativos que te acercarán a las causas de los problemas de tu PC

Nicolás Velásquez Espinel



Pro Evolution Soccer 2008

Programación: *Konami*
Distribuidor: *Konami*
Plataforma: *Playstation 3*
Calificación: *Mayores de 3 años*
http://www.konami-pesclub.com/pes2008



Con la nueva temporada de fútbol ya es tradición recibir las nuevas entregas de las dos grandes sagas de videojuegos del deporte rey. Hace tiempo que quedaron muy marcadas las preferencias de los usuarios por los FIFA y los PES, si bien esta última saga ha quedado como referencia a la hora de jugabilidad y ha ido ganando adeptos y resonancia publicitaria.

A pesar de que desde sus inicios la saga Pro Evolution Soccer se ha querido desmarcar de su gran competidor, ha ido actualizándose cada vez con mayor regularidad, a fin de seguir recortándole cuota de usuarios. Lo cual no quiere decir que ni FIFA ni PES hayan sacado todos los años nuevas entregas sin apenas cambios. No siempre ha sido así. Eso sí, en el caso de los PES, con una fórmula con pocos errores, a priori poco quedaba por cambiar. Pero eso no se puede tener en cuenta, y menos con nuevas consolas en las casas de los usuarios. No solo hay que aprovechar la nueva tecnología para un mayor despliegue audiovisual, hay que demostrar que se está usando en favor de la jugabilidad y, en este caso, del mayor realismo.

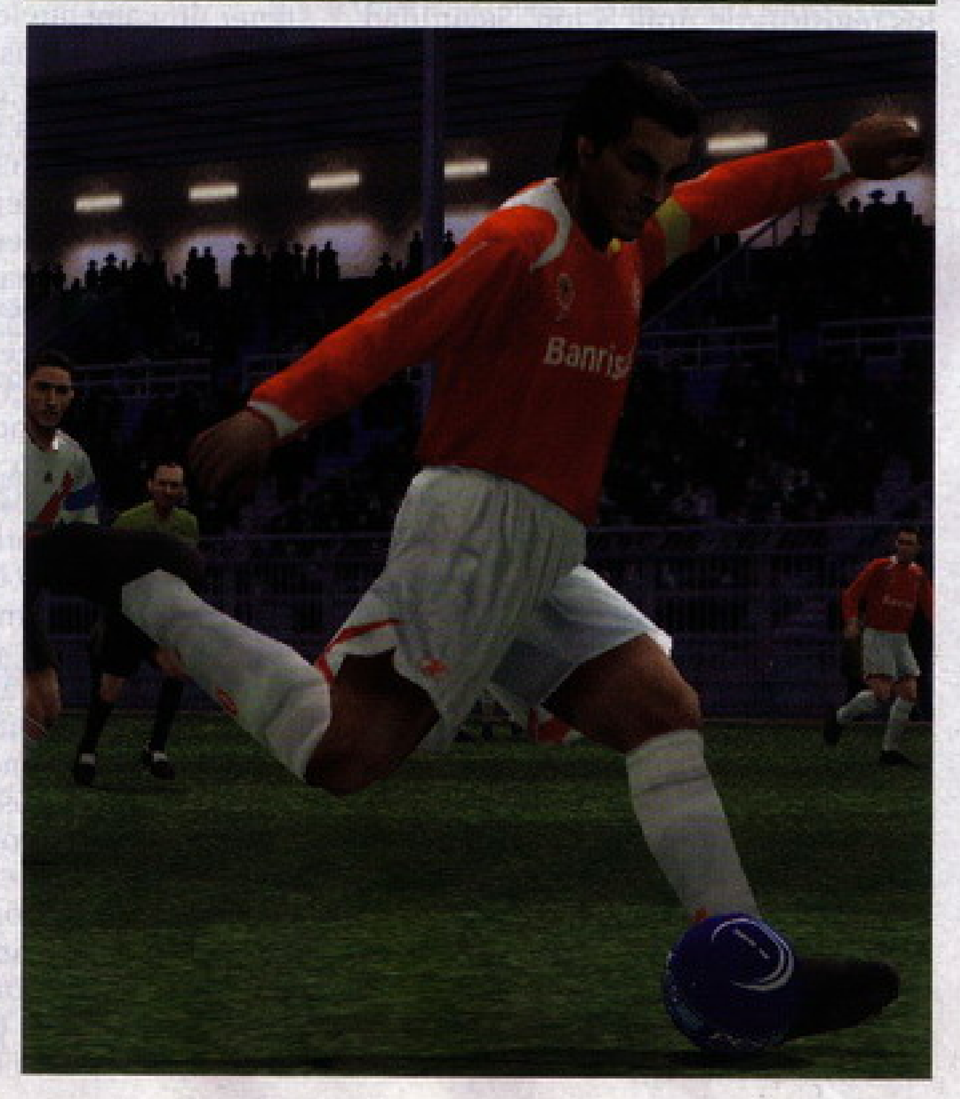


Porque cuando se tiene un juego como PES, de calidad contrastada en cuanto a jugabilidad, está claro que lo que se puede seguir mejorando es el realismo. Realismo en varios frentes: la recreación fiel de estadios, jugadores, licencias y torneos. Y realismo también en cuanto a más y mejores movimientos de los jugadores, tanto de los famosos como de los que no lo son tanto. En PES 2008 hay más de 3.000 jugadores licenciados y más de 250 equipos: hay más clubes reales de ligas europeas, y se han incorporado las selecciones nacionales de más países.

Por otro lado, su creador Seabass ha introducido por fin el esperado sistema de inteligencia artificial Teamvision, una de sus grandes metas para las nuevas entregas de PES. Con esta tecnología, la CPU se adaptará a nuestra manera de jugar, de forma que no podamos usar siempre las mismas jugadas y los mismos toques, dando un toque de improvisación que los amantes del fútbol "de fantasía" demandaban.

No faltan los nuevos movimientos, y los gráficos mejorados. Algo que notaremos incluso en la versión de la incombustible PS2, una consola que demuestra que todavía tiene algo que decir en ventas, más allá de nuevos Buzz y SingStar. Aunque el juego se está publicitando de forma masiva para la nueva generación de consolas, la versión de PS2 es sencillamente soberbia, y con el parque de consolas todavía funcionando a pleno pulmón, es muy probable que las ventas sorprendan a más de uno. Y es que, sea la versión que sea, PES 2008 es uno de los juegos del año, guste o no el fútbol.

	9
	9
	9
	10
	9
TOTAL	9





Sega Rally

Programación: *Sega Racing Studio*
Distribuidor: *Sega*
Plataforma: *Playstation 3*
Calificación: *Mayores de 3 años*
http://rally.sega-europe.com/es/





Sega Rally es una de las licencias más queridas por los fans de la compañía. No se ha prodigado tanto como otras sagas, y puede que por eso mismo siga siendo una marca de prestigio para Sega, una firma que sigue reconvirtiéndose y tratando de estabilizarse. Estabilizarse en su trayectoria como desarrollador multiplataforma, una estrategia que le ha dado resultados desiguales, pero que la siguen manteniendo entre las grandes. No con el pedigrí de antaño, pero Sega sigue siendo una compañía a la que no se debe despreciar ni perder la vida.

Sega Rally en sus inicios fue otro destello de genialidad de sus creadores, que supieron mezclar ingredientes de forma magistral para un arcade antológico. En los comienzos de la era de los 32 bits, sus dotes sentaron cátedra y no pocos simuladores de rally posteriores bebieron de la fuente de Sega Rally. Y es que el juego de Sega era algo más que una recreativa, tenía la ambición suficiente para enganchar a los jugones que quisieran más profundidad. Para muchos la cumbre de la saga fue Sega Rally 2, primero en recreativa y luego en una excelente versión para Dreamcast. Curiosamente, hoy parece que son muchos los que quieren desacreditar una estupenda conversión, que fue además uno de los mejores juegos de la primera hornada de la consola blanca de Sega. Sin embargo, la jugabilidad de Sega Rally 2 sigue completamente vigente actualmente. Y su adicción.

Tras un desapercibido Sega Rally 2006 para PS2 que no llegó a nuestras fronteras, Sega anunció la "reinvención" de su juego de rallies. Algo similar a lo que hizo hace unos años con OutRun, incluso programado por el mismo equipo que creó los impecables OutRun 2 y OutRun 2006. Es decir, una apuesta bastante segura con una fórmula que ya ha demostrado su éxito. Es más, Sega ha creado el denominado Sega Racing Studio para continuar en el futuro con nuevas entregas y más "reinvenciones" de sus sagas de conducción, así como la creación de nuevas franquicias del género.

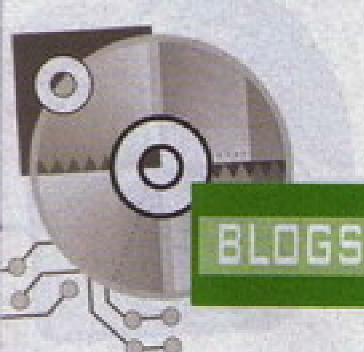
Sega ha hecho coincidir el lanzamiento de su nuevo Sega Rally con una nueva generación de consolas, algo así como una declaración de intenciones: un nuevo Sega Rally para una nueva era. La cuestión es si realmente ha habido un cambio radical en la saga. Y la respuesta es no. Sega Rally sigue siendo un arcade de rallies. Con elementos nuevos, pero no ha renunciado a sus raíces, y tampoco tendría mucho sentido que lo hiciera. No es un juego que deba competir con un Colin McRae: DiRT, por ejemplo. A fin de cuentas, Sega Rally es un notable arcade de conducción. Se han incluído algunas novedades para añadirle un poco más de sustancia al resultado, entre lo que destaca un significativo aumento del número de coches para elegir. Habrá que ir desbloqueando contenidos a medida que avancemos, pero supone una interesante mejora disponer de muchos más coches que en anteriores entregas. La idea, lógicamente, es que cada coche tenga un comportamiento propio, alejándose un poco del puro arcade para acercarse levemente a la simulación.



Otro de los detalles más llamativos es el efecto de deformación del terreno. El objetivo de Sega Racing Studio es que ni el coche ni el circuito tengan el mismo comportamiento o incidencia durante todas las vueltas. Si frenamos demasiado en ciertas partes del trazado, o levantamos demasiado barro o nieve, lo notaremos la próxima vez que pasemos por ahí. Sega Rally tiene otros pequeños detalles de este tipo, para hacer la experiencia arcade más variada y algo menos previsible. El juego es en resumen un regreso encomiable, algo lejos de la excelencia de la Sega de toda la vida, pero no deja de tener el gusto de los buenos arcades de conducción.

	8	■■■■■■■■
	7	■■■■■■■
	8	■■■■■■■■
	8	■■■■■■■■
	8	■■■■■■■■
TOTAL	8	■■■■■■■■





estilo web 2.0

Ya conoces todos los detalles de la web 2.0. La utilizas a diario en la red. Ya es hora de que actualices tu sitio aplicando su peculiar estilo.

La Web 2.0 ha supuesto una revolución, de la que ya formamos parte todos los internautas, ha marcado un antes y un después en cuanto a la forma que tenemos de interactuar con la información. Este concepto se refleja también en unas normas gráficas y de estilo que debes seguir, para hacer que tu sitio adquiera esa imagen moderna y dinámica que tanto nos gusta ver en la red.

Para que puedas conseguirlo, de una forma más fácil, aquí tienes unos pequeños consejos a tener en cuenta a la hora de diseñar, o elegir entre diseños confeccionados por otros. Así tus plantillas u hojas de estilo lucirán radiantes.

1. Diseño simple

El diseño debe ser sencillo y claro. No sólo debes escapar de los elementos superfluos, sino que tienes que tender a dejar sólo lo importante.

Una composición centrada, simple y con máximo tres columnas es la mejor opción. Separas las secciones de cada página mediante manchas de color y esquinas redondeadas.

2. Crea marca

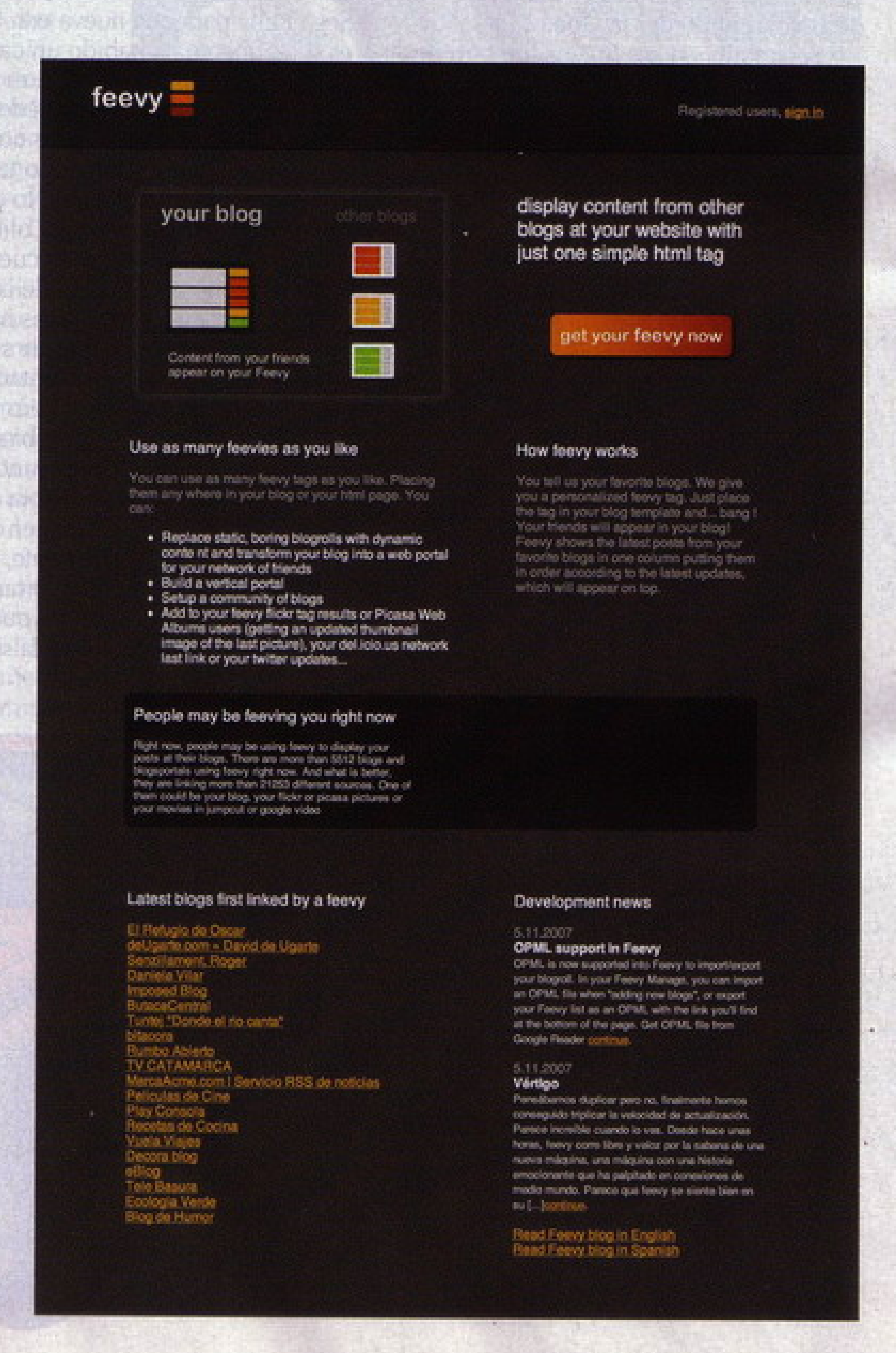
El medio sigue siendo el mensaje, para ello potencia tu imagen de marca.

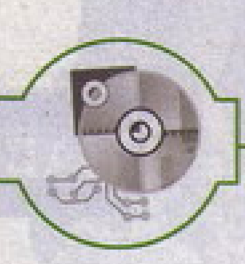
Diferencia claramente la cabecera del resto de la página, y coloca en ella tu logo, Este debe ser grande, claro y simple. La célebre broma entre diseñadores que afirma que el cliente siempre quiere el logo más grande, aquí se hace obligatorio.

El nombre de la Web debería ser una única palabra o a lo sumo dos, llamativa y lo más fácil de recordar posible.

3. Facilita la navegación

Tus visitantes vienen por tus contenidos. Debes ofrecerles todas las facilidades para poder llegar a ellos, de una forma clara y rápida. Un menú de navegación en la parte superior de la Web es clave. Que se vea y que se sepa en









qué sección se encuentra el visitante en cada momento.

4. Colores impactantes

Selecciona colores saturados con fuertes contrastes entre ellos. Pero recuerda que un poco de color es mucho. Si no quieres marear a tus visitantes, coloca colores claros o incluso blanco para dar descanso de las zonas importantes potenciadas.

5. Sensaciones de tridimensionalidad

Abusa de degradados dentro de la misma gama de un color, es decir de azul claro a oscuro, o a otro color. Potencia el despegue de los elementos claves a través de pequeñas sombras paralelas, biseles y reflejos en botones. Estos deben ser grandes, con leyenda breve. Incorpora también efectos de reflejo bajo algunas imágenes.

6. Destaca y brilla

Destaca tu sitio mediante un logo con un icono significativo y claro. Puedes utilizar iconos simbólicos, pero deben ser contundentes y claramentes identificativos.

Utiliza círculos dentados y rectángulos para colocar elementos del título.

7. Texto más grande y estructurado

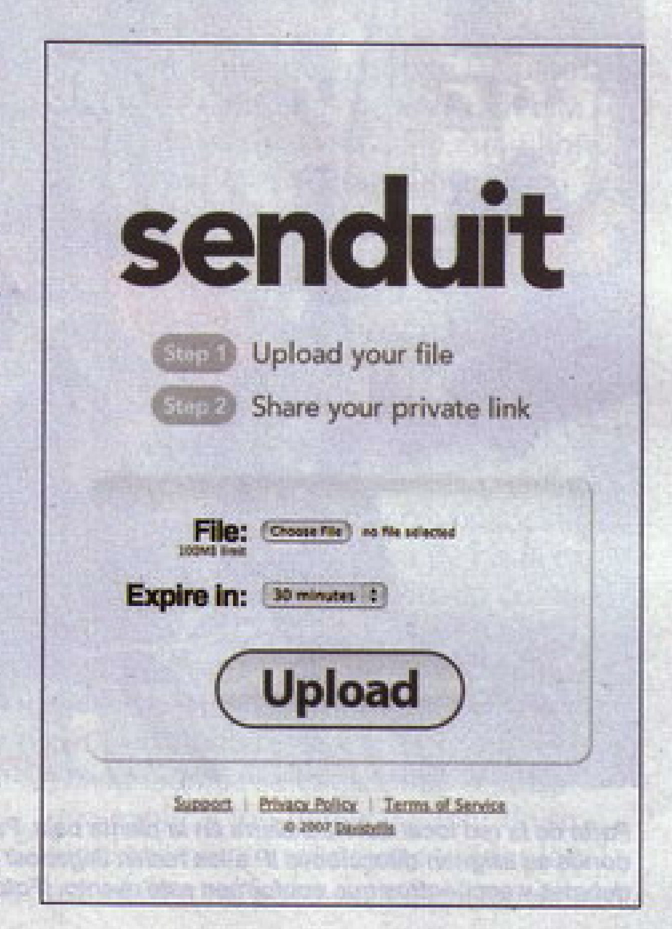
Facilita la lectura aumentando el tamaño de la letra de tu sitio. A la gente le costará menos leerlo y más gente llegará a la parte baja de la página.

Coloca pequeños cintillos estructurando el texto por temas. Y no olvides colocar una pequeña introducción en una tipo mayor, así como instrucciones o procedimientos de actuación de tus visitantes.

8. Beta

¡Ah! Y no olvides colocar el aviso de que tu Web está en fase beta. (Bueno, esto último es una broma, aunque en la práctica podría ser cierto).

Mon Magan
monmagan.com





Hackmeeting 2007

La magia del hackelarre

Desafiando a la inquisición las brujas realizaban encuentros clandestinos en los que compartir sus conocimientos, crear comunidad alrededor del fuego danzante, y explorar en comunión los designios del medievo. El país vasco fue, como muchos otros lugares, testigo de esta magia sumergida en la oscuridad impuesta por el poder de la Iglesia. Este año el histórico enclave de Guernica devolvía a la historia un Hackelarre al descubierto: un encuentro anual de hacktivistas que año tras año viene creando un espacio-tiempo ciberpunk en el que compartir conocimientos y recetas, conjuros y hechizos para transformar y combatir las sombras inquisidoras de la dominación tecnológica en favor de la libre circulación del conocimiento. El Hackmeeting 2007 dio cita una vez más a activistas, hackers, investigadoras y estudiantes de todos los rincones para re-ensamblar de forma colaborativa el poder del hacktivismo.



Parte de la red local del Hackelarre en la planta baja. Para conectarse a la red existe un DHCP humano donde se asignan direcciones IP a los recién llegados: una invitación a engancharse a la red de charlas, debates y encuentros que conforman este evento. [Foto tomada de Indymedia Estrecho, CC-by-sa]

Okupando la imaginación: de la fábrica de armas de destrucción a la fábrica del conocimiento libre

El pasado puente de Octubre cientos de hacktivistas se reunían en la antigua fábrica de armas Astra de Gernika; hoy un edificio okupado por la imaginación de los jóvenes del pueblo para dar cabida a eventos autogestionados de todo tipo. La fábrica de armas, abandonada en 1998, se encuentra reconvertida en fábrica de iniciativas sociales y cultura participativa desde el 2005. Una semana antes del evento empezaron a llegar hasta allí activistas de toda la península con el objetivo de acondicionar el espacio para abrir las puertas al octavo Hackmeeting, evento que en Italia ha cumplido su décima edición1, en Chile su segunda y se empieza a extender también por los EEUU.

Nada más llegar sorprende la arquitectura del sistema operativo del encuentro, embebido en las tres plantas del enorme edificio. "La distribución del espacio es importantísima" comenta Marga "ya que define la arquitectura de la participación y este evento es sobre

todo participativo, aquí no hay diferencia entre organizadoras y organizados". La planta baja a la que se accede por una enorme puerta se abre al caos autoorganizado. Un punto de información coordina todo el funcionamiento, las tareas, turnos y materiales del evento. Allí se acoge también a los recién llegados y el "DHCP humano" asigna a cada asistente una dirección IP para la red local. Y es que el Hackmeeting se comprende a sí mismo como una red distribuida, no sólo en relación a los puntos de acceso y los cables que cuelgan de las paredes de la planta baja (en la que más de medio centenar de ordenadores conforman una red local) sino también en relación al funcionamiento del evento. En la planta baja no podía faltar barra de bar (en la que tienen lugar muchas de las charlas y debates improvisados más interesantes) ni tampoco el clásico espacio "chillout" para relajarse y charlar tranquilamente o la zona reservada para comedor (atendido esta vez por un colectivo vegano de Bilbao que cocinó exquisitamente para más de cien personas durante el largo fin de semana).

En la planta intermedia había tres grandes espacios reservados para las charlas y talleres. Cada uno de estos espacios contaba con un ordenador reciclado, proyector y equipo de sonido dispuesto todo ello para sacar el máximo provecho al software libre y grabar las charlas a través del programa Audacity y enviarlas por red al servidor local y a la radio. Finalmente la última planta estaba se encontraba un gran dormitorio con espacio para un centenar de personas y varias salas pequeñas. En una de ellas se instaló el Centro de Medios, donde se gestionaban la relación con la prensa y se editaban los materiales de vídeo y audio, así como el servidor principal FTP, el enlace a Internet y el proxy-caché de Debian. Junto al Centro de Medios, un pequeño estudio de radio[2] permitía recopilar las charlas y documentar el evento con innumerables entrevistas y debates.

Una red de Nodos para que fluya el conocimiento

Como todos los años el hackmeeting se construye como una red de actividades (nodos) que van desde charlas y talleres hasta debates y juegos[3]. Cualquier persona puede proponer un nodo para el hackmeeting para compartir conocimientos, y proyectos o simplemente para ensamblar ideas y circuitos integrados con



la participación de los presentes. Uno de los nodos que más impacto causó fue la "Debianización" del PC de la barra del centro social por parte del "Comando Escamot Espiral" que, mediante un elaborado ritual, con montaje audiovisual incluido, conjuró a los espíritus del software libre pare exorcizar a Windows. Pero la magia del Hackelarre se condensó con mayor intensidad en el la sesión de brainhacking práctico, una propuesta de "viaje por los suburbios de la mente"[4] que dejó a más de un escéptico asombrado por las posibilidades de hackear nuestras mentes.

> **EL HACKMEETING SE COMPRENDE A SÍ MISMO COMO UNA RED DISTRIBUIDA, NO SÓLO EN RELACIÓN A LOS PUNTOS DE ACCESO Y LOS CABLES QUE CUELGAN DE LAS PAREDES DE LA PLANTA BAJA (EN LA QUE MÁS DE MEDIO CENTENAR DE ORDENADORES CONFORMAN UNA RED LOCAL) SINO TAMBIÉN EN RELACIÓN AL FUNCIONAMIENTO DEL EVENTO**

Los hechiceros de la seguridad informática tampoco faltaron al evento. Entre otros nodos destaca el de Txipi, que realizó una brillante introducción a la seguridad en VoIP[5] con un continuo despliegue de llamadas a sí mismo, a su contestador automático y escuchando su propia voz al otro lado del teléfono; despertando no pocas carcajadas en el público, al tiempo que los paquetes VoIP viajaban por la pantalla y eran esnifados en vivo por diversos programas. Durante la charla se profundizó en las cuestiones más importantes relacionadas con la seguridad VoIP, se describió la implementación sencilla de un sistema de VoIP con sofware libre (Asterisk + ATA), las vulnerabilidades de estas redes y las posibles medidas de protección.

El abogado y activista pro-copyleft David Maeztu expuso una propuesta de reforma de la LPI orientada hacia aquellas personas que no se sienten satisfechas con las opciones que se proponen desde Creative Commons y desean que sea posible que las obras entren en el Dominio Público de manera anticipada. Allí se encontraba también Javier de la Cueva, unos de los hacktivistas más conocidos del derecho español en favor del copyleft, y el final de la charla derivó en un interesante intercambio de los retos que aún pendientes para alcanzar la libre circulación de cultura y conocimientos.

Las herramientas de software libre para movimientos sociales ocupan un espacio importante en todo Hackmeeting. En esta ocasión hubo una presentación, a cargo de Martintxo, de la aplicación libre SomaSuite que permite la automatización de emisiones de radio. En ella se explicó la experiencia de la radio libre Garraxi Irratia (en Altsasu, Navarra)6 con este software y explicó su funcionamiento y ventaja a los asistentes. Entre ellos se encontraba Baku, principal desarrollador del programa, que durante el hackmeeting adaptó y recompiló el código de SomaSuite para que pudiera ser ejecutado en ordenadores viejos, tipo Pentium II, como los que reciclan y reutilizan muchos colectivos sociales sin grandes recursos. Otra de las herramientas que se ha consolidado como recursos fundamental en la red para la creación y organización participativa es sin duda MediaWiki, la plataforma de código libre que da soporte a Wikipedia. David Gómez se encargó de realizar una explicación-demostración[7] de su funcionamiento sobre un servidor local y asombró a no poco de los asistentes con

esta herramienta que supera ya los límites de su diseño y permite explorar infinidad de posibilidades imprevistas e innovadoras para la inteligencia colectiva.

En fin, resulta imposible resumir los más de treinta nodos que tejieron una red de conocimiento y experiencias libres y colectivas durante todo el hackmeeting. Para quienes no pudieron asistir al Hackmeeting de este año el intenso trabajo de la radio digital y el Centro de Medios permite acceder a las grabaciones y documentación diversa de todos los nodos del Hackmeeting en la página web del Hackelarre.

Autogestión, sinergias locales y semillas del futuro

El evento tuvo considerable resonancia en medios locales. Pudieron leerse reportajes de doble página en los dominicales de los principales periódicos de ámbito autonómico y también las radios, tanto libres como convencionales, emitieron entrevistas en directo y diferido con diferentes participantes[9]. Pero el impacto del Hackelarre no se agotó en los medios de comunicación ni en la red. Las calles de Gernika presenciaron la ya tradicional manifestación hacktivista de todos los años, un divertido pasacalles que reclama la defensa de la libre circulación de la cultura y el conocimiento. Durante el recorrido no faltaron voces de solidaridad con el portal "alasbarricadas.org" que ha sido recientemente multado con más de 6.000 € por injurias vertidas por un usuario anónimo contra el cantante y cabeza visible de la SGAE[10], Ramoncín. "Una sentencia sin precedentes" comentaba Didac desde el hackmeeting "que amenaza a la libertad de expresión en la red, sobre todo si es contra los órganos de poder del copyright más restrictivo".

Uno de los principales fines de estos encuentros es el dejar "huella" allá donde se celebran, en forma de impulso colectivo y recursos para la comunidad local. En este sentido la primera asamblea del nuevo laboratorio hacker de



El Hackmeeting 2007 se realizó en el Centro Social Okupado y Autogestionado de Gernika, antigua fábrica de armas Astra abandonada y reconvertida en espacio de alternativas culturales y sociales. [fotomontaje de EVhAck a partir de fotos de Indymedia Estrecho y Euskalherria, CC-by-sa]

Gernika no se ha hecho esperar. El hacklab ha adoptado el nombre Hackelarre en recuerdo del encuentro y ya se encuentra a cargo del servidor de radio del centro social para que Gernika cuente con un recurso tecnológico comunicativo libre, autogestionado y al servicio de la gente de la calle.

Un año más el Hackmeeting se consolida como espacio de confluencia de movimientos sociales, conocimientos informáticos y cultura ciberpunk. Nuevos cuerpos y máquinas se unen año tras año haciendo posible un relevo generacional que mantiene y mejora este proceso organizativo de código abierto. La preparación del siguiente hackmeeting hierve ya en la lista de correo[11] abierta a la participación de cualquier internauta dispuesto a beber del brebaje colectivo y experimentar "mucha pluralidad con muchas cosas en común", como dice elduende, un joven que asistió este año al hackmeeting por primera vez. Y no será la última.

EVhAck (evhack.info@gmail.com)

Enlaces

[1] http://www.hackmeeting.org/[2] http://www.sindominio.net/hackmeeting/index.php/2007/Radio
[3] http://www.sindominio.net/hackmeeting/index.php/2007/Nodos
[4] http://www.sindominio.net/hackmeeting/index.php/2007/Nodos/Brain_hacking_practico
[5] http://www.slideshare.net/txipi/seguridad-en-voip-hackelarre/download
[6] http://www.sindominio.net/garraxi/biltegi/presentacion-garraxi/presentacion-garraxi.odp
[7] http://sindominio.net/hackmeeting/index.php/2007/Nodos/Mediawiki/material
[8] http://www.sindominio.net/hackmeeting/index.php/2007/gal2007
[9] http://www.sindominio.net/hackmeeting/index.php/2007/gal2007#Grabaciones_sonoras_y_radios
[10] http://www.alasbarricadas.org/sgae/?page_id=7
[11] https://listas.sindominio.net/mailman/listinfo/hackmeeting